Volume 7, Issue 6, November 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

John F. Delaney
Adam Fleisher
Shawn Henry
Julie O'Neill
Anthony M. Ramirez
Aaron Rubin
Kelsey Spector
Joshua Stein
Nathan Taylor
Nikita Tuckett
Grant Schrader

FOLLOW US

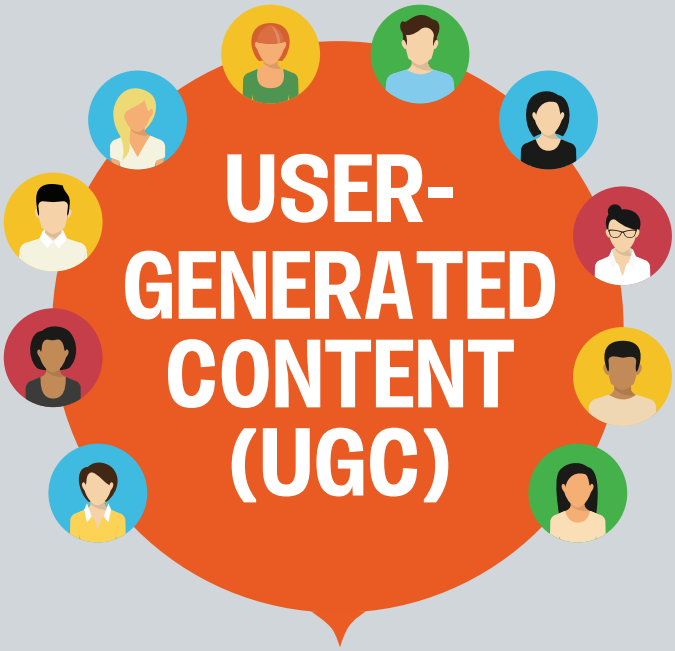
Morrison & Foerster's Socially Aware Blog

@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 provide five tips for reducing potential liability exposure in seeking to exploit user-generated content; we examine a Ninth Circuit decision highlighting the control that social media platform operators have over the content and data that users post to those platforms; we discuss five questions that companies should ask themselves to help prepare for a ransomware attack; we explore a controversial California court decision that narrows an important liability safe harbor for website operators; we review a federal court decision that illustrates the importance of securing clear and affirmative assent to electronic contracts; we take a look at some recent enforcement actions that indicate a shift toward requiring clearer and potentially more burdensome disclosures from companies engaged in interest-based advertising; and we examine a recent Northern District of California decision holding that a mobile app developer was not be liable under the Telephone Consumer Protection Act for a text initiated by one of the app's users.

All this—plus an infographic illustrating the impact of incorporating user-generated content in marketing campaigns.



Content provided by consumers, often reflecting their experiences with a brand

78% of marketers use UGC as part of their **marketing efforts.**[1]

57% of the marketers who avoid using UGC avoid it because they are concerned about violating **copyright law.**[1]

93% of consumers find UGC helpful in **making purchases.**[2]

Millennials

40%

trust information from UGC 40% more than information from traditional forms of media.[3]

Consumers

90%

spend 90% more time on websites that host UGC.[4]

Social Media

50%

campaigns incorporating UGC inspire **50% more engagement** than those without UGC.[4]

SOURCES

1. https://socialmediaweek.org/blog/2016/06/key-stats-best-practices-millennials-user-generated-content/
2. http://www.adweek.com/socialtimes/why-consumers-share-user-generated-content-infographic/639636
3. http://corp.crowdtap.com/socialinfluence
4. http://info.offerpop.com/rs/395-YDY-479/images/5ThingsYouDidntKnowAboutOP.pdf

COMMERCIALIZING USER-GENERATED CONTENT: FIVE RISK REDUCTION STRATEGIES

By John Delaney and Anthony Ramirez

We're in the midst of a seismic shift in how companies interact with user-generated content (UGC).

For years, companies were happy simply to host UGC on their websites, blogs and social media pages and reap the resulting boost to their traffic numbers. And U.S. law—in the form of Section 512(c) of the Digital Millennium Copyright Act (DMCA)—accommodated this passive use of UGC by creating a safe harbor from copyright damages for websites, blogs and social media platform operators that hosted UGC posted without the authorization of the owners of the copyrights in such UGC, so long as such operators complied with the requirements of the safe harbor.

Increasingly, companies are no longer satisfied with passively hosting UGC. Rather, they now want to find creative ways to commercialize such content, by incorporating it into ads (including print, TV and other offline ads), creating new works based on such content and even selling such content. Yet, in moving beyond mere hosting to proactive exploitation of UGC, companies risk losing the benefit of the DMCA Section 512(c) safe harbor, which could result in potentially significant copyright liability exposure.

For example, if a company finds that users are posting potentially valuable UGC to the company's Facebook page, or on Twitter in connection with one of the company's hashtags, that company may want to make such UGC available on its own website. The DMCA Section 512(c) safe harbor, however, is unlikely to protect the company in copying such UGC from the Facebook or Twitter platform to its own website.

The reality is that any company seeking to monetize or otherwise exploit UGC needs to proceed with extreme caution. This is true for several reasons:

- **UGC can implicate a wide range of rights . . .** As with any content, UGC is almost certainly subject to copyright protection, although certain tweets and other short, text-only posts could potentially be exempt from copyright protection if they qualify as "short phrases" under the Copyright Act. If any individuals are identifiable in UGC, then rights of publicity and rights of privacy may also be relevant. In addition, UGC may contain visible third-party trademarks or comments that defame or invade the privacy of third parties.

- **. . . and a wide range of rightsholders.** Notably, many of the rights necessary to exploit UGC are likely to be held by individuals and corporations *other than* the

posting user. For example, unless a photo is a "selfie," the photographer and the subject of the photo will be different individuals, with each holding different rights—copyright, for the photographer, and the rights of publicity and privacy, for the subject—that could be relevant to the exploitation of the photo. Moreover, any trademarks, logos and other images contained in a photo could potentially implicate third-party rightsholders, including third-party corporations. Videos also raise the possibility of unauthorized clips or embedded music.

- **If the UGC is hosted by a third-party social network, it may have Terms of Service that help—*or hurt*—efforts to exploit the UGC.** Most social media networks collect broad rights to UGC from their users, although they differ substantially when it comes to passing those rights along to third parties interested in exploiting the content. For example, if a company uses Twitter's Application Programming Interface (API) to identify and access Tweets that the company would like to republish, then Twitter grants to that company a license to "copy a reasonable amount of and display" the Tweets on the company's own services, subject to certain limitations. (For example, Twitter currently prohibits any display of Tweets that could imply an endorsement of a product or service, absent separate permission from the user.) Instagram also has an API that provides access to UGC, but, in contrast to Twitter, Instagram's API terms *do not appear to grant any license to the UGC* and affirmatively require companies to "*comply with any requirements or restrictions*" imposed by Instagram users on their UGC.

With these risks in mind, we note several emerging best practices for a company to consider if it has decided to exploit UGC in ways that may fall outside the scope of DMCA Section 512(c) and other online safe harbors. Although legal risk can never be eliminated in dealing with UGC, these strategies may help to reduce such risk:

The reality is that any company seeking to monetize or otherwise exploit UGC needs to proceed with extreme caution.

1. CAREFULLY REVIEW THE SOCIAL MEDIA PLATFORM TERMS

If the item of UGC at issue has been posted to a social media platform, determine whether the Terms of Service for such platform grants any rights to use such posted UGC off of the platform or imposes any restrictions on such content. Note, however, that any license to UGC granted by a social media platform almost certainly will not include any representations, warranties or indemnities, and so such a license may not offer any protection against third-party claims arising from the UGC at issue.

2. SEEK PERMISSION

If the social media platform's governing terms don't provide you with all of the rights needed to exploit the UGC item at issue (or even if they do), seek permission directly from the user who posted the item. Sophisticated brands will often approach a user via the commenting or private messaging features of the applicable social media platform and will present him or her with a link to a short, user-friendly license agreement. Often, the user will be delighted by the brand's interest in using his or her content. Of course, be aware that the party posting the content may not be the party that can authorize use of that content, as Agence France Presse learned the hard way in using photos taken from Twitter.

3. MAKE AVAILABLE TERMS AND CONDITIONS FOR "PROMOTIONAL" HASHTAGS

If a company promotes a particular hashtag to its customers, and would like to use content that is posted in conjunction with the hashtag, the company could consider making available a short set of terms alongside its promotion of that hashtag. For example, in any communications promoting the existence of the hashtag and associated marketing campaign, the company could inform customers that their use of the hashtag will constitute permission for the company to use any content posted together with the hashtag. Such an approach could face significant enforceability issues—after all, it is essentially a form of "browsewrap" agreement—but it could provide the company with a potential defense in the event of a subsequent dispute.

4. ADOPT A CURATION PROCESS

Adopt an internal curation process to identify items of UGC that are especially high-risk, which could include videos, photos of celebrities, photos of children, professional-quality content, any content containing copyright notices, watermarks and so forth and any content containing potentially defamatory, fraudulent or otherwise illegal content. Ensure that the curators are trained and equipped with checklists and other materials approved by the company's legal department or outside counsel. Ideally, any high-risk content should be subject to the company's most stringent approach to obtaining permission and clearing rights—or perhaps avoided altogether.

5. ADJUST THE APPROACH FOR HIGH-RISK USES

Consider the way in which the UGC at issue is expected to be used and whether the company's risk tolerance should be adjusted accordingly. For example, if an item of UGC will be used in a high-profile advertisement, the company may want to undertake independent diligence on any questionable aspects of the UGC,

even after obtaining the posting user's permission—or perhaps avoid any questionable UGC altogether.

In a social media age that values authenticity, more and more companies—even big, risk-adverse Fortune 100 companies—are interested in finding ways to leverage UGC relevant to their business, products or services. Yet the shift from merely hosting UGC to actively exploiting it raises very real legal hurdles for companies. The tips above are not a substitute for working closely with experienced social media counsel, but they collectively provide a framework for addressing legal risks in connection with a company's efforts to commercialize UGC.

NINTH CIRCUIT CASE DEMONSTRATES THAT THE SOCIAL MEDIA PLATFORM, NOT THE USER, IS IN CONTROL

by Aaron Rubin and Kelsey Spector

We have written before about website operators' use of the federal Computer Fraud and Abuse Act (CFAA) to combat data scraping. We have also noted a number of recent cases in which courts held that social media platforms, rather than the users of those platforms, have the right to control content on and access to the relevant websites. A recent Ninth Circuit decision, *Facebook v. Power Ventures*, brings these two trends together.

Power Ventures, the defendant, operated a website that aggregated users' content, such as friends lists, from various social media platforms. In an attempt to increase its user base, Power Ventures initiated an advertising campaign that encouraged users to invite their Facebook friends to Power Ventures' site.

Specifically, an icon on the Power Ventures site gave users the option to "Share with friends through my photos," "Share with friends through events" or "Share with friends through status" and displayed a "Yes I do" button that users could click. If the user clicked the "Yes I do" button, Power Ventures would create an event, photo or status on the user's Facebook profile. In some cases, clicking the button also caused an email to be sent to the user's friends "from" Facebook stating that the user had invited them to a Facebook event.

But the case can also be seen as an example of social media operators exerting the right to control their platforms, and the content and data that users post to those platforms, even against the users' own wishes.

Upon becoming aware of this activity, Facebook sent Power Ventures a cease and desist letter informing Power Ventures that it had violated Facebook's terms of use and demanding that Power Ventures stop soliciting Facebook users' information. Facebook also blocked Power Ventures' IP address from accessing Facebook. When Power Ventures changed its IP address and continued to access the site, Facebook sued, alleging among other things that Power Ventures had violated the CFAA. As we discussed at greater length in our previous article, the CFAA imposes liability on anyone who "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer."

In analyzing Facebook's CFAA claim, the court reasoned that Power Ventures did not access Facebook's computers without authorization initially because "Power users arguably gave Power permission to use Facebook's computers to disseminate messages" and, accordingly, "Power reasonably could have thought that consent from Facebook users to share the promotion was permission for Power to access Facebook's computers." That all changed, however, when Facebook sent Power Ventures the cease and desist letter expressly rescinding whatever authorization Power Ventures may have otherwise had. According to the court, "[t]he consent that Power had received from Facebook users was not sufficient to grant continuing authorization to access Facebook's computers after Facebook's express revocation of permission."

The court employed a colorful analogy to support its reasoning:

> Suppose that a person wants to borrow a friend's jewelry that is held in a safe deposit box at a bank. The friend gives permission for the person to access the safe deposit box and lends him a key. Upon receiving the key, though, the person decides to visit the bank while carrying a shotgun. The bank ejects the person from its premises and bans his reentry. The gun-toting jewelry borrower could not then reenter the bank, claiming that access to the safe deposit box gave him authority to stride about the bank's property while armed. In other words, to access the safe deposit box, the person needs permission both from his friend (who controls access to the safe) and from the bank (which controls access to its premises). Similarly, for Power to continue its campaign using Facebook's computers, it needed authorization both from individual Facebook users
>
> (who controlled their data and personal pages) and from Facebook (which stored this data on its physical servers).

Accordingly, the court held that, following receipt of Facebook's cease

and desist letter, Power Ventures intentionally accessed Facebook's computers knowing that it was not authorized to do so, making Power Ventures liable under the CFAA.

On one level, *Facebook v. Power Ventures* can be seen as a battle between two competing social media platforms over valuable user data. Certainly it is easy to understand why Facebook would object to Power Ventures poaching Facebook's data. But the case can also be seen as an example of social media operators exerting the right to control their platforms, and the content and data that users post to those platforms, even against the users' own wishes.

In this sense, one can place *Facebook v. Power Ventures* in the line of recent cases holding that, at the end of the day, it is the social media platform operator and not the user that controls the platform. And that is an important fact for individuals and companies to keep in mind when they are investing time and money to establish and maintain a social media presence on a platform controlled by someone else.

FIVE QUESTIONS TO HELP PREPARE FOR A RANSOMWARE ATTACK

by Nathan Taylor and Shawn Henry

The news has been filled this year with reports of ransomware attacks against companies and government agencies, including even law enforcement. Ransomware refers to a type of malware that encrypts or otherwise restricts access to a machine or device. As part of the attack, the attacker will demand that the victim pay a ransom in order to receive the encryption key or otherwise recover access to the compromised machine.

The reality is that ransomware attacks have been proliferating against all types of companies and organizations. Ransomware is a profitable business for underground circles, and we expect to see continued targeting. Because these attacks may be isolated to a single machine, they frequently do not impact a company's business continuity or result in a noticeable service disruption. In response to an infection, companies may be able to obtain the technical assistance needed to defeat the attack. Free online resources exist that will identify which ransomware infected your system and provide victims with known decryption keys. In other cases, companies may determine that the data loss is not significant and/or that backups exist, allowing them to rebuild the computer by reformatting the hard drive and reinstalling a clean operating system, applications and data. In other cases, though, companies pay the ransom.

Ransomware attacks have been proliferating against all types of companies and organizations.

Ransomware attackers frequently use many of the same tools and tactics, such as spear phishing, as other hackers. Unlike many hackers, however, ransomware attackers are not focused on stealing data that can be sold or used for illicit purposes (e.g., credit card information and trade secrets). Instead, ransomware is about economic extortion. The attackers prevent a company from being able to access its own system or data, and they make a demand. Usually, they want money, but that could change. Imagine a hacker who holds data and systems hostage in return for the company's releasing a public statement, making a divestiture or arranging for a senior executive's departure? The distinction between routine malware and ransomware is important to manage the scope of the threat. While some companies may not maintain data that is of value to cyber thieves (although that is becoming less and less the case, as evidenced by the proliferation of W-2 tax information phishing attacks), every company is a potential target of a ransomware attack.

There are a couple of reasons why this is such a challenging problem to overcome from a technology perspective. Once the files are encrypted, it is nearly impossible to decrypt them. This leaves the affected organization facing the difficult choice of either paying the ransom or losing their data. In many cases, downtime and data loss are more costly than the ransom, which is why many organizations opt to pay. The second major challenge is that ransomware is highly polymorphic. There are tens of thousands of malware samples and variants detected in the wild.

Ransomware is a profitable business for underground circles, and we expect to see continued targeting.

As a result, all companies should be mindful of the risk of such an attack and take steps to limit the impact of such an attack, including being prepared to respond.

Responding to a ransomware attack can be a stressful and unnerving experience. Not surprisingly, depending on the system that is the target of the attack, time is usually of the essence. As part of a company's broader incident response preparation, it is worth anticipating what you would do in the event of a ransomware attack. The following five questions are a good starting point for companies, and

in-house counsel might consider leading this review together with their information security managers. While the answers to these questions often differ depending on the nuance or nature of a given attack, the investment in planning related to these questions can reduce the stress and increase the agility and effectiveness of a company's response to an attack.

1. WILL YOU PAY THE RANSOM?

This literally can be the million-dollar question, although ransom demands historically have been much smaller. For example, it is common to see ransom demands between $500 and $50,000, typically to be paid with Bitcoin. Regardless of the extortion level, many companies have taken the approach of not negotiating with blackmailers or otherwise paying ransom, regardless of the situation. In fact, the FBI does not encourage payment.

Still, even where there is a general (and understandable) resistance to paying ransom, the answer to this question for most companies will depend on the impact and timing of the attack. That is, the answer frequently depends on the business continuity risk and service disruption potential that the attack presents, as well as whether there is an available and useful backup of the data/service maintained by, or hosted on, the impacted system. More specifically, how badly does your company need the impacted system or the data stored on that system?

For example, if a company cannot access a machine that has critical data for which there is no adequate or available backup, or if the machine is integral to business operation (e.g., a web server or payment service) and there are challenges in replacing the machine in a timely manner, a company may determine that it has little choice but to pay the ransom because the costs of lost access far outweigh the ransom demand. In many scenarios, however, companies have elected not to pay the ransom because they have a sufficient backup of data maintained on the machine or because the lost access to the system does not have a meaningful business impact. For example, from a business continuity perspective, there may be no practical difference between a ransomware attack that locks an employee's company-issued laptop and the physical theft of that laptop.

Significantly, paying does not always result in the hackers making good on their promise. In a recent case, a hacker only provided partial access to a hospital's encrypted data before asking for more money to complete the deal. At that point, the hospital refused.

2. WHAT SYSTEMS ARE SUBJECT TO THE GREATEST RISK (AND ARE THEY PROTECTED)?

The first question highlights the critical, yet obvious, point that the potential impact of a ransomware attack all depends on which machine, system or device is hit. It also highlights the fact that ransomware is not just an information security issue but also a business continuity issue (not unlike, for example, natural disasters). On this point, a company should have the advantage over a ransomware attacker.

Specifically, a company can assess its systems and dependencies and identify those that present the greatest risk to the company in the event of a ransomware attack. In fact, most companies with business continuity plans will have already gone through this exercise in a more general context. Regardless, once you have identified systems that are critical to your company's ongoing operations, you then can consider how those systems are currently protected from the types of malware typically deployed in a ransomware attack and whether additional protections make sense. In addition to having appropriate data backup and recovery plans in place, common information security considerations include:

- The use of robust endpoint detection and response (EDR) solutions,
- Taking advantage of application white-listing,
- Restricting user permissions and access controls,
- Implementing software restriction policies (SRP),
- Ramping up efforts to detect spear-phishing emails and
- Disabling macros from running in files that are received in email or downloaded from websites.

3. DO YOU HAVE SUFFICIENT BACKUPS?

While the previous question was focused on the extent to which critical systems are protected, this question is focused on contingency planning in the event that a company is the victim of a successful ransomware attack. If critical systems are impacted by ransomware, how will your company respond, and will you be able to continue (somewhat) normal business operations? This is an important question, even if your company would consider paying the ransom. For example, even if a company pays the ransom, there will be a loss of data or availability until the key is received and, hopefully, normal access is restored. As a result, from both a data and a systems perspective, it is important to determine the extent of a company's backups and alternatives that can support business operations. A company should consider not only the extent of its backups, but how frequently those backups are created and tested and whether the backups themselves are susceptible to being encrypted or deleted by the hacker. This will help determine the scope of the data loss at risk in the event of an attack. Similarly, a company should consider its process

for restoring data from backup (or switching to backup systems) and whether that process can be simplified or made more efficient.

4. WILL YOU MAKE THE ATTACK PUBLIC?

It can be helpful to consider whether, or the circumstances when, your company would make public that it has been the victim of a ransomware attack. Most companies that have gone public with the fact that they were the victim of an attack appeared to do so because the attack significantly impacted their normal business operations and there was a delay in restoring those operations.

If normal business operations are impacted, there is a question of how you communicate that fact to customers, vendors, business partners and the public generally. For example, if a company will pay the ransom and expects to restore operations within a relatively short time but feels that it is important to communicate to relevant third parties that certain systems are down, does the communication have to highlight the cause of the issue, or can it simply identify the impact? For example, a company could indicate that it is aware of the problem, that it is working to address the problem and when it expects the issue to be resolved. While the nuance of an attack (e.g., the impact and duration) is incredibly important to answering this question, the answer can be equally nuanced. For example, a company may elect to alert third parties only where there is a contractual requirement to do so, keeping in mind that a ransomware attack typically does not include a data breach. Regardless, it a company must consider its communication strategy in the event of an attack. Some companies may even want to take the next step and prepare standby statements that can be used, if needed, for example, in response to a third party, or even an employee, revealing the incident.

5. WILL YOU CONTACT LAW ENFORCEMENT?

A question companies frequently consider in the context of a ransomware attack (and cybersecurity incidents generally) is whether to contact law enforcement and, if so, which law enforcement agency. The answer will be company-specific and depend on a number of factors. Nonetheless, it is important for a company to identify and understand the reasons why it would contact law enforcement in the event of an attack. Not surprisingly, the likelihood of achieving the desired objective varies significantly based on the reason for contacting law enforcement.

A company may contact law enforcement because it wants the attacker brought to justice or because it hopes that there may be technical assistance that law enforcement can provide to help the company regain control of the relevant machine (and avoid paying the ransom). While the facts are always critical, these may not be the primary reasons to contact law enforcement because the likelihood of law enforcement catching what is likely a foreign actor may be slim; similarly, law enforcement may not have the capability to crack the encryption, and the facts may not warrant law enforcement investing resources in that effort.

A company, however, may contact law enforcement for other reasons. For example, a company may contact law enforcement because, if the attack becomes public, the company can reassure customers, vendors, business partners or even regulators that it did everything possible to respond to the attack. For many types of public cybersecurity incidents, it has become standard for a company to indicate that it has notified law enforcement and is cooperating with the investigation. This also highlights the fact that the company is a victim. In some instances, a company may contact law enforcement because its cyber response policies indicate that law enforcement should be contacted or because it has become standard practice for the company in responding to cyber incidents. A company may also contact law enforcement because the company believes that "it is the right thing to do" as a good corporate citizen. Finally, a company's cyber insurance policy may require that suspected crimes be reported to law enforcement in order to make a claim for coverage. For each of these reasons, a company may conclude that it shall contact law enforcement, even though it believes that the criminal will not ultimately be caught.

The question of which law enforcement agency to contact is heavily dependent on the facts, including the type of company impacted, the threat actor, the type of machine impacted and the nature of that impact; a detailed discussion is beyond the scope of this article. For example, if a significant ransomware attack impacts critical infrastructure or a federally regulated entity (e.g., a national bank or an airline), the company should contact federal law enforcement, such as the FBI. If a ransomware attack hits a small hardware store, however, the company should instead consider contacting local law enforcement or using online reporting through the Internet Crime Complaint Center at www.ic3.gov.

MOVING FORWARD

Unfortunately, ransomware is costing businesses hundreds of millions of dollars annually, whether in the form of payments, intrusion response or both. By definition, you cannot prepare after an event. By asking and answering these five questions early enough, you can arrive at a risk posture that is suitable for your business. Hopefully you will never experience a problem. However, should a ransomware incident occur, you will have increased options for managing the event and quickly getting back to business.

This piece was originally shared on Corporate Compliance Insights and is republished here with permission.

CONTROVERSIAL CALIFORNIA COURT DECISION SIGNIFICANTLY NARROWS A CRUCIAL LIABILITY SAFE HARBOR FOR WEBSITE OPERATORS

by John Delaney and Joshua Stein

A recent California court decision involving Section 230 of the Communications Decency Act (CDA) is creating considerable concern among social media companies and other website operators.

As we've discussed in past blog posts, CDA Section 230 has played an essential role in the growth of the Internet by shielding website operators from defamation and other claims arising from content posted to their websites by others.

Under Section 230, a website operator is not "treated as the publisher or speaker of any information provided" by a user of that website; as a result, online businesses such as Facebook, Twitter and YouTube have been able to thrive despite hosting UGC on their platforms that may be false, deceptive or malicious and that, absent Section 230, might subject these and other Internet companies to crippling lawsuits.

Recently, however, the California Court of Appeal affirmed a lower court opinion that could significantly narrow the contours of Section 230 protection. After a law firm sued a former client for posting defamatory reviews on Yelp.com, the court not only ordered the former client to remove the reviews, but demanded that Yelp (which was not party to the dispute) remove these reviews.

The case, *Hassell v. Bird*, began in 2013 when attorney Dawn Hassell sued former client Ava Bird regarding three negative reviews that Hassell claimed Bird had published on Yelp.com under different usernames. Hassell alleged that Bird had defamed her, and, after Bird failed to appear, the California trial court issued an order granting Hassell's requested damages and injunctive relief.

In particular, the court ordered Bird to remove the offending posts, but Hassell further requested that the court require Yelp to remove the posts because Bird had not appeared in the case herself. The court agreed, entering a default judgment and ordering Yelp to remove the offending posts. (The trial court also ordered that any *subsequent* comments associated with Bird's alleged usernames be removed, which the Court of Appeal struck down as an impermissible prior restraint.) Yelp challenged the order on a variety of grounds, including under Section 230.

The Court of Appeal held that the Section 230 safe harbor did not apply and that Yelp could be forced to comply with the order. The court reasoned that the order requiring Yelp to remove the reviews did not impose any liability on Yelp; Yelp was not itself sued for defamation and had no damages exposure, so Yelp did not face liability as a speaker or publisher of third-party speech. Rather, citing California law that authorized a court to prevent the repetition of "statements that have been adjudged to be defamatory," the court characterized the injunction as "simply" controlling "the perpetuation of judicially declared defamatory statements." The court acknowledged that Yelp could face liability for failing to comply with the injunction, but that would be liability under the court's contempt power, not liability as a speaker or publisher.

The *Hassell* case represents a significant setback for social media companies, bloggers and other website operators who rely on the Section 230 safe harbor to shield themselves from the misconduct of their users. While courts have previously held that a website operator may be liable for "contribut[ing] materially to the alleged illegality of the conduct"—such as StubHub.com allegedly suggesting and encouraging illegally high ticket resale prices—here, in contrast, there is no claim that Yelp contributed to or aided in the creation or publication of the defamatory reviews, besides merely providing the platform on which such reviews were hosted.

Of particular concern for online businesses is that *Hassell* appears to create an end-run around Section 230 for plaintiffs who seek to have allegedly defamatory or false UGC removed from a website: sue the suspected posting party and, if that party fails to appear, obtain a default judgment; with a default judgment in hand, seek a court order requiring the hosting website to remove the objectionable post, as the plaintiff was able to do in the *Hassell* case.

Commentators have observed that *Hassell* is one of a growing number of recent decisions seeking to curtail the scope of Section 230. After two decades of expansive applications of Section 230, are we now on the verge of a judicial backlash against the law that has helped to fuel the remarkable success of the U.S. Internet industry?

COURT UPHOLDS ENFORCEABILITY OF "CLICKWRAP" EMPLOYEE AGREEMENT

by Nikita Tuckett and Aaron Rubin

As we have previously discussed, if you want your electronic contracts to be enforceable, it is a best practice to require the counterparty to affirmatively accept the contract by checking a box or clicking a button. A recent New Jersey district court decision, *ADP, LLC v. Lynch*, reinforces this point. Such issues most often arise in the context of website terms of use, but *ADP v. Lynch* involved

a non-competition provision and forum selection clause contained in documentation presented to employees electronically in connection with stock option grants.

The employer, ADP, sued two former employees for taking jobs at a competitor in violation of certain restrictive covenants contained in the stock option grant documentation. The employees sought to dismiss the action on the basis of lack of jurisdiction, and ADP responded by pointing to a forum selection clause in the grant documentation. The employees argued, however, that they had not received adequate notice of the restrictive covenants and that the forum selection clause was unenforceable.

The grant documentation containing the restrictive covenants and the forum selection clause had been presented to the employees in electronic form, and, based on the allegations in ADP's complaint, the employees were required to acknowledge the documentation in order to receive the stock option grants. Specifically, ADP had presented the documentation in such a way that each employee was physically unable to click the required "Accept Grant" button unless he or she had affirmatively checked a prior box indicating that he or she had read the associated documents containing the restrictive covenants and forum selection clause.

The court also noted that ADP's manager of its stock plan services "provided a step-by-step rundown" of the process that employees were required to follow to accept stock option grants and that, "in order to accept those awards, an employee would have to affirmatively acknowledge that he or she reviewed the Restrictive Covenants before proceeding." This illustrates another point we have noted previously: If you want your electronic contracts to be enforceable, you should not only make sure to implement them in a way that requires affirmative acceptance, but you should also be prepared to produce evidence that the user at issue actually accepted.

In light of the above, the court analyzed the grant documentation containing the restrictive covenants and forum selection clause as an enforceable "clickwrap" contract similar to the website terms of use at issue in another case we have written about previously, *Fteja v. Facebook, Inc.*:

> At this stage in the litigation, the Court finds that the forum selection clauses are encompassed by enforceable clickwrap agreements. The complaints unequivocally allege that an employee could not accept any stock grants until acknowledging that he or she reviewed all grant documents, including the Restrictive Covenants that contained the forum selection clauses. [...] In order to accept those awards, an employee would have to affirmatively acknowledge that he or she reviewed the Restrictive Covenants before proceeding. [...] Therefore, this case involves the type of clickwrap agreement that other courts have found to be enforceable.

The court also found unpersuasive the employees' argument that mutual assent was lacking because the acknowledgment box did not expressly state "I agree to the terms of the grant documents" but instead merely required the employees to acknowledge that they had read those documents. According to the court, this was a "distinction without difference" because, in accepting the option grant, the defendants were required to represent as part of the grant agreements that they had read the restrictive covenant agreements.

Accordingly, as ADP sufficiently alleged that it had required the employees to affirmatively accept the restrictive covenants and forum selection clause as part of the electronic contracting process, the court denied the employees' motion to dismiss.

While it does not necessarily break new ground in terms of the enforceability of electronic contracts, this case does illustrate that the same principle applies whether you are seeking to impose terms and conditions on users of your website or enforce restrictive covenants and a forum selection clause in an employment agreement: make sure the counterparty is required to take some clear and affirmative action to expressly accept the contract.

INTEREST-BASED ADVERTISING DISCLOSURE REQUIREMENTS BECOME CLEARER—AND POTENTIALLY MORE BURDENSOME

by Julie O'Neill and Adam Fleisher

Recent enforcement decisions within the digital advertising industry indicate a shift in—and a clarification of—the required disclosures for companies engaged in interest-based advertising (IBA).

In particular, these decisions, taken together, indicate that an app developer's link to its privacy policy at the point of app download may be deemed *insufficient*, unless the link *points directly to the IBA disclosure section of the policy or there is a clear link at the top of the policy that directs the user to that section*.

Further, these decisions suggest that companies that comply with the digital advertising industry's IBA self-regulatory principles *should expressly affirm such compliance in their privacy policies*.

BACKGROUND

Some quick background: IBA is the collection of information about users' online activities across different websites or mobile applications, over time, for the purpose of delivering online advertising to those users based on those activities. Although it is an important part of the

online ecosystem, if not done right, IBA can raise privacy concerns among consumers, who may feel that they are being spied upon by advertisers.

The Digital Advertising Alliance (DAA) has worked to ensure that IBA is done right. The DAA is a consortium of media and marketing associations that, in an effort to ward off legislation, has designed and implemented a self-regulatory compliance regime that seeks to address the Federal Trade Commission's (FTC) IBA notice and choice expectations. The principles underlying this compliance regime are set out in the DAA's *Self-Regulatory Principles* ("DAA Principles"). The DAA enforces these principles through the IBA accountability program, run by the Council of Better Business Bureaus and the Direct Marketing Association.

The DAA self-regulatory program is, at its heart, a notice-and-choice regime. In short, to facilitate such notice and choice, the DAA provides an advertising option icon to be placed in or near an online interest-based ad. By clicking on the icon, a consumer is sent to a landing page that describes the data collection practices associated with the ad and provides an opt-out mechanism.

Importantly, however, the DAA Principles have also been interpreted by the IBA accountability program to require "enhanced" notice on any website where information is *collected* for IBA purposes. In response to this interpretation, website publishers typically provide such notice in the form of an "Our Ads" or similarly named link in the site footer, separate from the privacy policy link, that clicks through to the same landing page as the advertising option icon or to similar notice and choice information.

THE RECENT DECISIONS

In its recent enforcement actions, the IBA accountability program appears to have exported this manifestation of the enhanced notice requirement to mobile applications, notwithstanding the provisions of the DAA's guidance on the *Application of Self-Regulatory Principles to the Mobile Environment*, first published in 2013.

Although it is an important part of the online ecosystem, if not done right, interest-base advertising can raise privacy concerns among consumers, who may feel that they are being spied upon by advertisers.

That guidance expressly provides that app publishers (i.e., "first parties") that permit third parties to collect information for IBA purposes must "provide a clear, meaningful, and prominent link to a disclosure that either points to a choice mechanism or setting that meets Digital Advertising Alliance specifications or individually lists such Third Parties." This notice must be provided in two separate locations:

- Either prior to download (e.g., in the app store on the application's page), during download, on first opening of the app *or* at the time cross-app data is first collected; *and*
- In the application's settings or any privacy policy.

The IBA accountability program appears, however, to be taking the position that a link to the privacy policy from the app store (or any other location) is *not enough* to meet this first prong. That is, a "clear, meaningful, and prominent link" to the IBA disclosure must be a link *directly* to the IBA section of the privacy policy, in the same way that the "Our Ads" or similarly named link in the site footer clicks through to the IBA section of the privacy policy.

The IBA accountability program's *Spinrilla* decision, for example, states that the accountability program could not find an "enhanced link notice separate from the privacy policy link" in the applicable app stores and affirmed that if only one privacy policy link will be used in the app store (where it is typically not possible to provide two separate links), "the link to the privacy policy must either go directly to the pertinent discussion of IBA or direct the user to that place through a clear link at the top of the privacy policy."

The other accountability program decisions, *Bearbit Studios* and *Top Free Games*, reaffirm this interpretation. In light of these decisions, app publishers may want to revisit how they provide "enhanced notice" of their IBA practices.

Finally, the Mobile Guidance states that first parties should "indicate adherence" to the DAA Principles in their privacy policies. The accountability program decisions noted the absence of this language in the companies' privacy policies, and the companies appear to have added language to their disclosures to comply with this obligation. Whether a company would want to affirmatively make this representation of its own accord is something that may warrant additional consideration, as the company's failure to fully comply with such a representation could give rise to a charge of deception under Section 5 of the FTC Act or a similar state law.

THE UPSHOT

In light of these developments, a company engaged in IBA should:

- If engaged in IBA with respect to one or more of its apps, review how it discloses its IBA practices at the point of app download; and
- Discuss with counsel the advisability of expressly stating adherence to the DAA Principles in its privacy policy.

APP DEVELOPER NOT LIABLE UNDER TCPA FOR USER-INITIATED TEXTS

by Grant Schrader

A recent decision out of the Northern District of California brings good news for developers of mobile apps that incorporate text messaging functions. Those functions may create the risk of claims under the Telephone Consumer Protection Act, which generally prohibits the delivery of a text message without the recipient's express consent. But in *Cour v. Life360, Inc.*, U.S. District Judge Thelton E. Henderson granted defendant Life360's motion to dismiss a putative TCPA class action after determining Life360 could not be held liable under the TCPA for a text initiated by a user of Life360's messaging and geolocation application.

BACKGROUND

The plaintiff alleged that he received a single, unsolicited text message from Life360, which operates a mobile application that allows users to text and see the location of fellow users on their contact lists. According to the plaintiff, after users download the application and set up an account, the application requests access to their contact lists so they can invite their friends and family to join. Users choose those in their contacts they wish to invite and then press an "Invite" button on the screen to send the invitations via text message. Users are not told how or when those invitations will be sent.

Plaintiff filed claims under the TCPA and California's Unfair Competition Law (UCL) on behalf of himself and a nationwide class of persons that received at least one text message from or on behalf of Life360. Life360 moved to dismiss both claims.

ONE TEXT SUFFICIENT TO CONFER STANDING UNDER *SPOKEO*

Life360 first argued that the plaintiff lacked Article III standing because he failed to allege a concrete injury, as required under the U.S. Supreme Court's decision in *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540 (2016). But the Court rejected that argument, holding that even though the plaintiff received only one text, the invasion of privacy it caused was sufficiently concrete to confer standing.

LIFE360 NOT LIABLE UNDER THE TCPA OR UCL

The key disagreement between the parties was whether Life360 or its user was responsible for "initiating" the invitational text message sent to the plaintiff. Relying on guidance from the Federal Communications Commission's July 2015 declaratory ruling, the Court ruled that the user—and not Life360—initiated the text to plaintiff, and thus Life360 could not be held liable.

The Court reasoned that Life360's users have to affirmatively choose which of their contacts will receive an invitation and then press the "Invite" button to actually send the invitations. Even though Life360 does not inform its users how or when those invitations will be transmitted, given the TCPA's purpose of preventing invasions of privacy, "the person who chooses to send an unwanted invitation is responsible for invading the recipient's privacy even if that person does not know how the invitation will be sent." Consequently, Life360 could not be held liable for the text message under either the TCPA or the UCL.

TAKEAWAY

As this case demonstrates, to mitigate the risk of TCPA liability, developers of messaging software or applications should ensure that any text messages sent through their platforms are initiated by the users themselves through their affirmative conduct.

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**.
