

SOCIALLY AWARE



2011 BEST LAW FIRM NEWSLETTER

THE SOCIAL MEDIA LAW UPDATE

IN THIS ISSUE

Peering Into the Future: Google Glass and the Law

Page 2

Ownership of Business-Related Social Media Accounts

Page 4

Two Circuits Address the First Amendment Status of Facebook Activity

Page 7

Collaborative Consumption – Is It Good to Share?

Page 9

Potential Limitations Placed on Unilateral Right to Modify Terms of Use

Page 12

A Warning for Websites Allowing Data Collection for Online Behavioral Advertising

Page 14

EDITORS

[John Delaney](#)
[Gabriel Meister](#)
[Aaron Rubin](#)

CONTRIBUTORS

[Patrick Bernhardt](#)
[Anelia V. Delcheva](#)
[Adam Fleisher](#)
[Reed Freeman](#)
[Benjamin Han](#)
[Jacob Michael Kaufman](#)
[Alistair Maughan](#)
[Susan McLean](#)
[Gabriel Meister](#)
[Aaron Rubin](#)
[Nathan Salminen](#)

FOLLOW US

 [Morrison & Foerster's Socially Aware Blog](#)

 [@MoFoSocMedia](#)

**MORRISON
FOERSTER**



In this issue of *Socially Aware*, our [Burton Award](#)-winning guide to the law and business of social media, we explore legal concerns raised by Google Glass; we provide an overview of the growing body of case law addressing ownership of business-related social media accounts; we take a look at two circuit court decisions addressing the interplay between social media usage and the First Amendment; we examine the trend toward collaborative consumption and associated legal issues; we discuss an important new decision regarding unilateral modifications to online terms of use; and we highlight an industry warning to website operators who collect data for purposes of online behavioral advertising.

PEERING INTO THE FUTURE: GOOGLE GLASS AND THE LAW

By [Gabriel Meister](#) and [Benjamin Han](#)



Google Glass Is Banned On These Premises

stopthecyborgs.org @ @ @ @

Sign offered by [Stop the Cyborgs](#) to indicate a 'no-Glass' zone. This image is licensed under a [Creative Commons Attribution-NonCommercial-NoDerivs 3.0 Unported License](#).

WHAT IS GOOGLE GLASS?

As most *Socially Aware* readers know, Google Glass (“Glass”) is a form of [wearable technology](#) that gives its users hands-free access to a variety of smartphone features by attaching a highly compact [head-mounted display](#) system to a pair of specially designed eyeglass frames. The display system connects to a smartphone via Bluetooth. In its current form, Glass can pull information from the web, take photographs, record videos, send messages via email or SMS, notify its user about messages and upcoming events and provide navigation directions via GPS. An embellished demonstration of Glass’s features is available at Google’s Glass [web page](#).

Although Glass is in the testing stage as of the time of this writing and boasts only a modest set of features, the device has caused quite a stir in both the mainstream and social media spheres. Wearable technology, however, has been around for quite a while

(for an extensive history of wearable computers, pay a visit to Paul Miller’s [article](#) on *The Verge*) and, although controversial, many of the concerns raised by Google Glass are not entirely new. This article will explore some of the more common concerns raised about Glass in the context of evolving legal and social norms — all premised on the assumption that Glass eventually will ultimately become a widely used, mainstream product.

GLASS AND PRIVACY

When the [original Kodak cameras](#) were released in the late 19th century, they caused a huge uproar among both lawmakers and consumers for their ability to do what they are designed to do: that is, [take pictures](#). This led to widespread bans on cameras at beaches, the Washington Monument and other locations. Samuel Warren and Justice Louis Brandeis aptly noted in an 1890 *Harvard Law Review* [article](#):

Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that “what is whispered in the closet shall be proclaimed from the house-tops.” For years there has been a feeling that the law must afford some remedy for the unauthorized circulation of portraits of private persons[.]

As Kodak cameras became more mainstream, society adapted by creating new laws, one of the most important of which was development of the “[reasonable expectation of privacy](#)” doctrine, which purports to protect individuals from being photographed in certain places recognized as “zones of privacy” — a designation that does not typically extend to public places.

Needless to say, Glass is made of more [advanced technology](#) than the original Kodak cameras, and this new technology raises a whole new set of

potential concerns. In particular, (1) taking a photograph with a traditional [camera](#) is typically more noticeable to subjects and onlookers alike than taking a photograph with a “wearable” device like [Glass](#), and (2) the Bluetooth connection between Glass and its user’s smartphone allows the possibility of [real-time facial recognition](#).

In part due to these concerns, on May 16, 2013, a bipartisan caucus of congressmen sent Google an [inquiry](#) regarding a variety of privacy matters. In response to that inquiry, Google [announced](#) on June 3, 2013, that it would not allow applications with facial recognition on Google Glass. (Naturally, hackers have [thumbed their noses](#) at Google’s announcement, reportedly building their own unauthorized software with facial recognition features.)

Although banning facial recognition apps may address the second concern noted above, the first concern still stands because people being photographed by a Glass wearer, whether in a “zone of privacy” or in a public place in which there is no reasonable expectation of privacy, simply might not even know it. A handful of establishments have responded by [preemptively banning](#) the device from their premises. Seattle’s 5 Point Café was, perhaps, the first to issue such a ban, [announcing](#) via

Only time will tell whether one-off bans on Glass and similar devices are akin to the overreactions — at least we now perceive them to be overreactions — that inspired bans on Kodak cameras in the late 19th century.

Facebook back in May 2013, “For the record, The 5 Point is the first Seattle business to ban in advance Google Glasses. And a** kickings will be encouraged for violators.” Colorado’s Press Play Bar followed with its own ban in July 2013. And Guantanamo has banned Google Glass.

Only time will tell whether one-off bans on Glass and similar devices are akin to the overreactions — at least we now perceive them to be overreactions — that inspired bans on Kodak cameras in the late 19th century. And, perhaps preemptively, Glass already limits a user’s ability to take photos to cases in which the user either speaks an audible command or makes a visible swipe on the device’s tactile sensor, and limits video recordings to 10 seconds in length without a user holding onto the tactile sensor. Of course, developers have already created an app that lets users take pictures by simply winking. Glass’s entrance into the mainstream is poised to cause further disruption.

BREAKING THE CASINO

In the 1960s, a group of UCLA and MIT graduate students created a “cigarette pack sized analog device” that increased the expected gain of playing roulette by 44%. The theory behind the device was to feed data concerning the motion of the roulette wheel and ball to a primitive computer that would predict the likely location of the ball’s drop. The premise of such a device was featured more recently in an episode of the popular television show CSI, in which (again) a pair of students created a device that would send video data from the casino back to an off-site computer run by one of the students, who would then relay the predictions back to the player on-site.

The possibility of improving gamblers’ odds over the house’s odds goes further than just roulette. For instance, with the assistance of a computer, even average blackjack players could accomplish feats reserved for the most skilled card counters; this is why Nevada gaming

regulators issued an alert to casino operators in February 2009, warning them about the use of a then newly released simple card counter app. Wearable computers at the poker table can even be used to transmit hand information from one play to another, enabling collusion.

Perhaps it’s only natural that casino operators are fearful of Google Glass. The Associated Press reported on June 12, 2013, that the Nevada and New Jersey Gaming Commissions have urged casinos to ban gamblers from wearing Google Glass on their premises. Some casino operators, such as Caesar’s Palace, have already forbidden their customers from wearing Glass while in their casinos, and Delaware has banned Glass from its own casinos. None of this is surprising, given casinos’ long history of taking strong measures to prevent players from gaining an edge over the house. And given the level of deference that state gaming commissions afford casinos in limiting the use of electronics on their premises, Glass is likely to be unwelcome at gambling houses for the foreseeable future.

Perhaps it’s only natural that casino operators are fearful of Google Glass.

SAFETY WHILE DRIVING

In February 2013, Sergey Brin, Google co-founder and Glass developer, commented during a segment of TED Talks that one of Project Glass’s goals was to change how people interact with their smartphones. According to Brin, the goal is to “free your hands” and “free your eyes” by limiting the need to look down at a phone screen. One Glass feature that best embodies this goal is turn-by-turn navigation.

In its current iteration, Glass’s turn-by-turn navigation is relatively simple, capable only of providing pop-up notifications of upcoming turns. In the future, Glass may be capable of layering information over a user’s peripheral vision, and even augmenting that information with information from the web. Yet, even in light of the device’s relatively simple set of current navigational features, the possibility of using Glass while driving has caused plenty of stir.

Daniel Simons and Christopher Chabris, psychology professors at the University of Illinois and Union College, respectively, explored the potential safety concerns arising from using Glass while driving in a May 24, 2013 New York Times op-ed piece. Simons and Chabris argue that people are fundamentally incapable of looking away from where they’re headed for more than a couple of seconds without losing their bearings. Drivers “intuitively grasp” this limitation by only glancing at the car radio or speedometer briefly before returning their eyes to the road. (Meanwhile, other distractions have been shown to be far more dangerous; the op-ed cites a study that demonstrated that drivers who texted with their mobile devices looked away from the road for as long as 4.6 seconds during a given six-second period, more than sufficient time to cause a major accident.)

Glass tries to circumvent this limitation by only displaying turn-by-turn information at relevant times, that is, just before turns that are coming up, as demonstrated in this video. Still, Simons and Chabris believe that it will be a challenge to find the right balance of information that can be safely displayed directly in drivers’ fields of vision.

Safety concerns like these are the motivation behind West Virginia State Rep. Howell’s proposed legislation that would amend driving laws to prohibit “using a wearable computer with head mounted display” while driving.

Delaware's lawmakers have introduced [similar legislation](#). And according to [some reports](#), the UK [Department for Transport](#) is considering its own ban on using Google Glass while driving.

It is unclear whether a blanket legal ban on head-mounted displays is the best approach to maximize safety. Arguably, Glass may strike the right balance by providing drivers with the same information they would typically retrieve by glancing down at a GPS system — without making drivers look away from the road. Head-mounted systems like Glass could be also used as a sort of “warning system” that alerts drivers that they are, say, approaching the speed limit, again without having to look down at separate speedometers. On the other hand, any guidelines for when and how head-mounted displays like Glass can be used on the road would probably need to be both granular and flexible to accommodate what will undoubtedly be a rapidly evolving technology.

THE FUTURE

Can you envision the first time someone uses Glass to surreptitiously record a feature film at the local multiplex? According to [Fast Company](#), a VP at the [National Association of Theatre Owners](#) has imagined just such a situation and says that his group anticipates working with its hundreds of members to develop Glass usage policies for their theaters. Can you picture the first time someone uses Glass to record a concert whose producer or venue enforces a strict “no videotaping” policy, or to secretly photograph sensitive documents containing trade secrets? Or the first time someone is wearing Glass while committing a crime? How will workplaces handle Glass, whether worn by visitors or used by their own employees on or off the job?

Countless situations are going to be influenced by Google Glass and similar wearable technologies. And given the range of issues that have already arisen in beta, these technologies' impact on laws and social norms is bound to be

more than just a matter of where you can or can't wear your Glass.

OWNERSHIP OF BUSINESS-RELATED SOCIAL MEDIA ACCOUNTS

By [Aaron Rubin](#) and [Anelia V. Delcheva](#)

Social media platforms have become an increasingly important means for companies to build and manage their brands and to interact with their customers, in many cases eclipsing companies' traditional “.com” websites. Social media providers typically make their platforms available to users without charge, but companies nevertheless invest significant time and other resources to create and maintain their presences on those providers' platforms. A company's social media page or profile and its associated followers, friends and other connections are often considered to be valuable business assets.

The message to companies who use social media is loud and clear: it is imperative to proactively establish policies and practices that address ownership and use of business-related social media accounts.

But who owns these valuable assets — the company or the individual employee who manages the company's page or profile? Social media's inherently interactive nature has created an important role for these individual employees. Such an

employee essentially acts as the “voice” of the company and his or her style and personality may be essential to the success and popularity of that company's social media presence. As a result, the lines between “company brand” and “personal brand” may become blurred over time. And when the company and the individual part ways, that blurring can raise difficult issues, both legal and logistical, regarding the ownership and valuation of business-related social media accounts.

Such issues have arisen in a number of cases recently, several of which we discuss below. Although these cases leave open a number of questions, the message to companies who use social media is loud and clear: it is imperative to proactively establish policies and practices that address ownership and use of business-related social media accounts.

PHONEDOG V. KRAVITZ

A recently settled California case, *PhoneDog v. Kravitz*, raised a number of interesting issues around the ownership and valuation of social media accounts. The defendant, Noah Kravitz, worked for the plaintiff, PhoneDog, a mobile news and reviews website. While he was employed by PhoneDog, Kravitz used the Twitter handle “@PhoneDog_Noah” to provide product reviews, eventually accumulating 17,000 Twitter followers over a period of approximately four and a half years. Kravitz then left PhoneDog to work for one of its competitors but he maintained control of the Twitter account and changed the account handle to “@noahkravitz.” When Kravitz refused PhoneDog's request to relinquish the Twitter account that had been previously associated with the “@PhoneDog_Noah” handle, PhoneDog filed a complaint against Kravitz asserting various claims, including trade secret misappropriation, conversion, and intentional and negligent interference with economic advantage.

Kravitz filed a motion to dismiss the complaint based on a number of arguments, including PhoneDog's

inability to establish that it had suffered damages in excess of the \$75,000 jurisdictional threshold. Kravitz also disputed PhoneDog's ownership interest in either the Twitter account or its followers, based on Twitter's terms of service, which state that Twitter accounts belong to Twitter and not to Twitter users such as PhoneDog. Finally, Kravitz argued that Twitter followers are "human beings who have the discretion to subscribe and/or unsubscribe" to the account and are not PhoneDog's property, and asserted that "[t]o date, the industry precedent has been that absent an agreement prohibiting any employee from doing so, after an employee leaves an employer, they are free to change their Twitter handle."

With respect to the amount-in-controversy issue, PhoneDog asserted that Kravitz's continued use of the "@noahkravitz" handle resulted in at least \$340,000 in damages, an amount that was calculated based on the total number of followers, the time during which Kravitz had control over the account, and a purported "industry standard" value of \$2.50 per Twitter follower. Kravitz argued that any value attributed to the Twitter account came from his efforts in posting tweets and the followers' interest in him, not from the account itself. Kravitz also disputed PhoneDog's purported industry standard value of \$2.50 per Twitter follower, and contended that valuation of the account required consideration of a number of factors, including (1) the number of followers, (2) the number of tweets, (3) the content of the tweets, (4) the person publishing the tweets, and (5) the person placing the value on the account.

With respect to the ownership issue, PhoneDog claimed that it had an ownership interest in the account based on the license to use and access the account granted to it in the Twitter terms of service, and that it also had an ownership interest in the content posted on the account. PhoneDog also

pointed to a purported "intangible property interest" in the Twitter account's list of followers, which PhoneDog compared to a business customer list. Finally, PhoneDog asserted that, regardless of any ownership interest in the account, PhoneDog was entitled to damages based on Kravitz's interference with PhoneDog's access to and use of the account, which (among other things) purportedly affected PhoneDog's economic relations with its advertisers.

It is worth noting that the case might have been more straightforward — and the result more favorable to the company — had PhoneDog established clear policies regarding the ownership of business-related social media accounts.

The court determined that the amount-in-controversy issue was intertwined with factual and legal issues raised by PhoneDog's claims and, therefore, could not be resolved at the motion-to-dismiss stage. Accordingly, the court denied without prejudice Kravitz's motion to dismiss for lack of subject matter jurisdiction. The court also denied Kravitz's motion to dismiss PhoneDog's trade secret and conversion claims, but granted Kravitz's motion to dismiss PhoneDog's claims of interference with prospective economic advantage.

The parties subsequently settled the dispute, so, unfortunately, we will never

know how the court would have ruled on the variety of interesting issues that the case presented. Interestingly, although the terms of the settlement remain confidential, Kravitz appears to have kept control of the Twitter account and its attendant followers. It is worth noting that the case might have been more straightforward — and the result more favorable to the company — had PhoneDog established clear policies regarding the ownership of business-related social media accounts.

ARDIS HEALTH, LLC ET AL. V. NANKIVELL

A New York case, *Ardis Health, LLC et al. v. Nankivell*, more clearly illustrates the fundamental point that companies should proactively establish policies and practices that address the ownership and use of business-related social media accounts.

The plaintiffs in *Ardis Health* were a group of closely affiliated online marketing companies that develop and market herbal and beauty products. The defendant was a former employee who had held a position at Ardis Health, LLC as a "Video and Social Media Producer." Following her termination, the defendant refused to turn over to the plaintiffs the login information and passwords for the social media accounts that she had managed for the plaintiffs during her employment. The plaintiffs then filed a lawsuit against the defendant and sought a preliminary injunction seeking, among other things, to compel her to provide them with that access information.

Fortunately for the plaintiffs, they had required the defendant to execute an agreement at the commencement of her employment that stated in part that all work created or developed by defendant "shall be the sole and exclusive property" of one of the plaintiffs, and that required the defendant to return all confidential information to the company upon request. This employment agreement also stipulated

that “actual or threatened breach . . . will cause [the plaintiff] irreparable injury and damage.” On these facts, the court noted that “[i]t is uncontested that plaintiffs own the rights to” the social media account access information that the defendant had refused to provide. Interestingly, the court held that the plaintiffs were likely to prevail on their conversion claim, effectively treating the disputed social media account access information as a form of intangible personal property. The court also determined that plaintiffs were suffering irreparable harm as a result of the defendant’s refusal to turn over that access information. Accordingly, the court granted the plaintiffs’ motion for a preliminary injunction ordering the defendant to turn over the disputed login information and passwords to the plaintiffs.

As far as we can tell from the reported decision in *Ardis Health*, the defendant’s employment agreement did not expressly address the ownership or use of social media accounts or any related access information. Nonetheless, even the fairly generic work product ownership and confidentiality language included in the defendant’s employment agreement, as noted above, appears to have been an important factor in the favorable outcome for the plaintiffs, which illustrates the advantages of addressing these issues contractually with employees — in advance, naturally. And as discussed below, companies can put themselves in an even stronger position by incorporating more explicit terms concerning social media accounts into their employment agreements.

EAGLE V. MORGAN AND MAREMONT V. FREDMAN

Former employers aren’t always the plaintiffs in cases regarding the ownership of business-related social media accounts. In an interesting twist, two other cases — *Eagle v. Morgan* and *Maremont v. Fredman* — were brought by employees who alleged that their employers had taken over and started

using social media accounts that the employees considered to be personal accounts.

Eagle began as a dispute over an ex-employee’s LinkedIn account and her related LinkedIn connections. The plaintiff, Dr. Linda Eagle, was a founder of the defendant company, Edcomm. Dr. Eagle alleged that, following her termination, Edcomm personnel changed her LinkedIn password and account profile, including by replacing her name and photograph with the name and photo of the company’s new CEO. Among the various claims filed by each party, in pretrial rulings, the court granted Dr. Eagle’s motion to dismiss Edcomm’s trade secret claim and granted Edcomm’s motion for summary judgment on Dr. Eagle’s Computer Fraud and Abuse Act (CFAA) and Lanham Act claims.

Regarding the trade secret claim, the court held that LinkedIn connections did not constitute trade secrets because they were “either generally known in the wider business community or capable of being easily derived from public information.” Regarding her CFAA claims, the court concluded that the damages Dr. Eagle claimed she had suffered — putatively arising from harm to reputation, goodwill and business opportunities — were insufficient to satisfy the “loss” element of a CFAA claim, which requires some relation to “the impairment or damage to a computer or computer system.” Finally, in rejecting the plaintiff’s claim that Edcomm violated the Lanham Act by posting the new CEO’s name and picture on the LinkedIn account previously associated with Dr. Eagle, the court found that Dr. Eagle could not demonstrate that Edcomm’s actions caused a “likelihood of confusion,” as required by the Act.

Eventually, the *Eagle* case proceeded to trial. The court ultimately held for Dr. Eagle on her claim of unauthorized use of name under the Pennsylvania statute that protects a person’s commercial

interest in his or her name or likeness, her claim of invasion of privacy by misappropriation of identity, and her claim of misappropriation of publicity. The court also rejected Edcomm’s counterclaims for misappropriation and unfair competition. Meanwhile, the court held for the defendants on Dr. Eagle’s claims of identity theft, conversion, tortious interference with contract, civil conspiracy, and civil aiding and abetting. Although the court’s decision reveals that Edcomm did have certain policies in place regarding establishment and use of business-related social media accounts by employees, unfortunately for Edcomm, those policies do not appear to have clearly addressed ownership of those accounts or the disposition of those accounts after employees leave the company.

Companies should consider clearly addressing the ownership of company social media accounts in agreements with their employees.

In any event, although Dr. Eagle did prevail on a number of her claims, the court concluded that she was unable to establish that she had suffered any damages. Dr. Eagle put forth a creative damages formula that attributed her total past revenue to business generated by her LinkedIn contacts in order to establish a per contact value, and then used that value to calculate her damages for the period of time when she was unable to access her account. But the court held that Dr. Eagle’s damages request was insufficient for

a number of reasons, primarily that she was unable to establish the fact of damages with reasonable certainty. The court also denied Dr. Eagle's request for punitive damages. Therefore, despite prevailing on a number of her claims, Dr. Eagle's victory in the case was somewhat pyrrhic.

In *Maremont*, the plaintiff, Jill Maremont, was seriously injured in a car accident and had to spend several months rehabilitating away from work. While recovering, Ms. Maremont's employer, Susan Fredman Design Group, posted and tweeted promotional messages on Ms. Maremont's personal Facebook and Twitter accounts, where she had developed a large following as a well-known interior designer. Although Ms. Maremont asked her employer to stop posting and tweeting, the defendant continued to do so. Ms. Maremont then brought claims against Susan Fredman Design Group under the Lanham Act, the Illinois Right of Publicity Act, and the Stored Communications Act, as well as a common law right to privacy claim. The parties filed cross-motions for summary judgment, which the court denied with respect to the Lanham Act and Stored Communications Act claims, largely due to lack of evidence on whether or not Ms. Maremont suffered actual damages as a result of her employer's actions. The court granted Susan Fredman Design Group's motion for summary judgment with respect to Ms. Maremont's right of publicity claim, based on the fact that the defendant did not actually impersonate Ms. Maremont when it used her accounts. The court also granted Susan Fredman Design Group's motion for summary judgment with respect to Ms. Maremont's right of privacy claim because the "matters discussed in Maremont's Facebook and Twitter posts were not private and that Maremont did not try to keep any such facts private."

PROACTIVE STEPS

Considering how vital social media accounts are to today's companies, and given the lack of clear applicable

law concerning the ownership of such accounts, companies should take proactive steps to protect these valuable business assets.

For example, companies should consider clearly addressing the ownership of company social media accounts in agreements with their employees, such as employee proprietary information and invention assignment agreements. Agreements like this should state, in part, that all social media accounts that employees register or manage as part of their job duties or using company resources — including all associated account names and handles, pages, profiles, followers and content — are the property of the company, and that all login information and passwords for such accounts are both the property and the confidential information of the company and must be returned to the company upon termination or at any other time upon the company's request. In general, companies should not permit employees to post under their own names on company social media accounts or use their own names as account names or handles. If particular circumstances require an employee or other individual to post under his or her own name — for example, where the company has engaged a well-known industry expert or commentator to manage the account — the company might want to go a step further and include even more specific contractual provisions that address ownership rights to the account at issue.

In parallel, companies should implement and enforce social media policies that provide employees with clear guidance regarding the appropriate use of business-related social media accounts, including instructions on how to avoid blurring the lines between company and personal accounts. (Keep in mind, however, that social media policies need to be carefully drafted so as not to not run afoul of the National Labor Relations Act, state laws restricting

employers' access to employees' personal social media accounts, or the applicable social media platforms' terms of use.) Finally, companies should control employee access to company social media accounts and passwords, including by taking steps to prevent individual employees from changing account usernames or passwords without authorization.

TWO CIRCUITS ADDRESS THE FIRST AMENDMENT STATUS OF FACEBOOK ACTIVITY

By Nathan Salminen

Two recent U.S. appellate court decisions have clarified the extent to which the First Amendment protects the social media activities of government employees. In *Gresham v. City of Atlanta*, the Court of Appeals for the Eleventh Circuit found that an individual's First Amendment interest in posting to Facebook is reduced when he or she configures such post to be private, while in *Bland v. Roberts*, the Court of Appeals for the Fourth Circuit held that Facebook "likes" constitute protected speech under the First Amendment. Although both decisions deal with the rights of government employees in particular, the decisions have relevance beyond government employees.

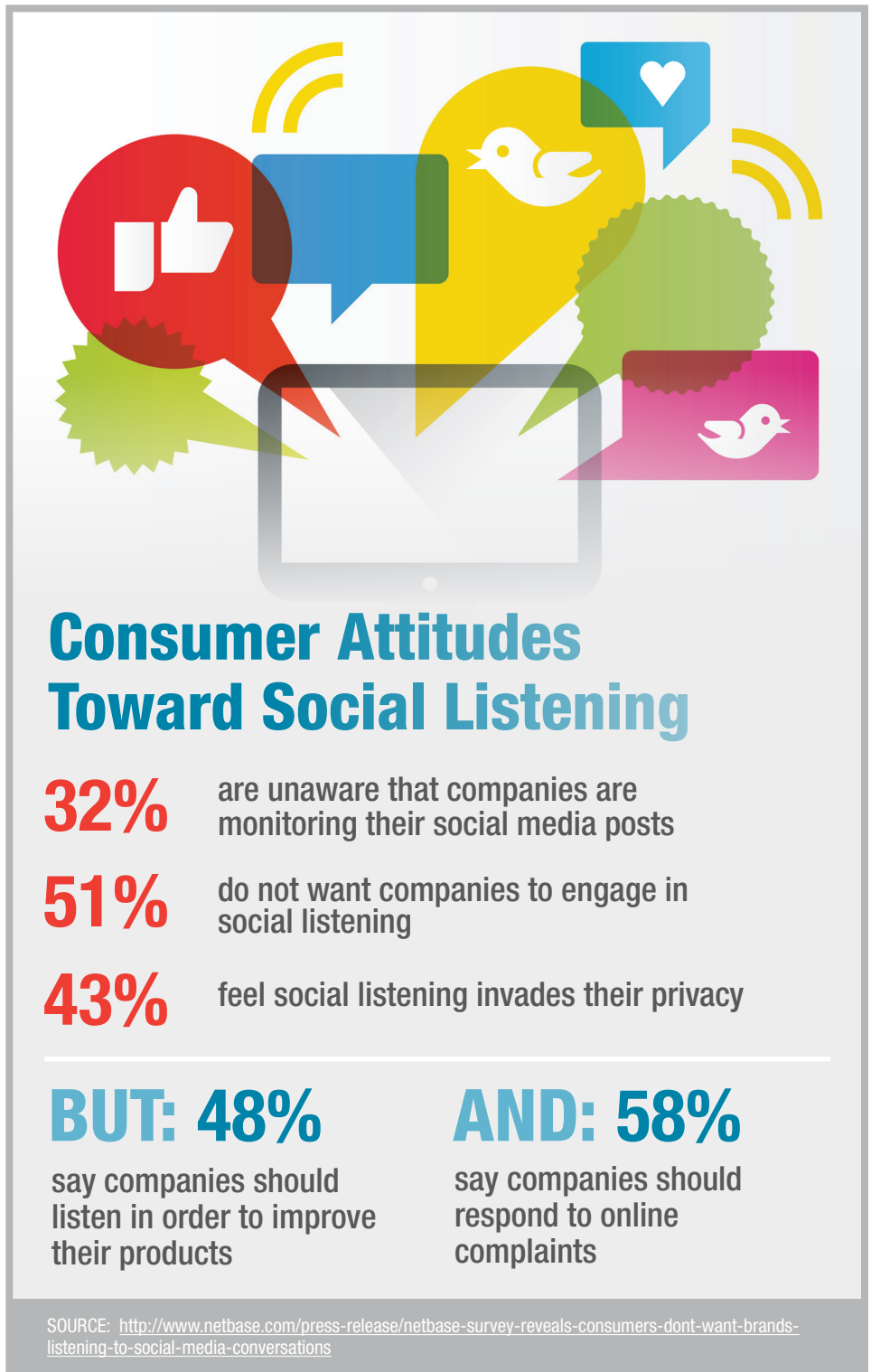
U.S. courts have long held that the government has a greater interest in restricting the speech of its employees than it does in restricting the speech of the citizenry in general. However, the government's ability to restrict the speech of its employees is limited by a test the U.S. Supreme Court outlined in *Pickering v. Board of Education* in 1968. The test requires that, in order for the employee to maintain

a successful First Amendment claim against his or her governmental employer, the employee must, among other things, show that he or she was speaking about a matter of public concern, and that his or her interest in doing so outweighs the government's interest in providing effective and efficient service to the public.

First Amendment protection for “likes”: *Bland v. Roberts*.

In August of 2012, we discussed the decision of a District Court in Virginia that a government employee “liking” a Facebook page was insufficient speech to merit constitutional protection. Deputies of the Hampton Sheriff’s Office alleged that they were terminated because they “liked” the campaign page of a candidate running against their boss, the current sheriff. While much of the suit dealt with the current sheriff’s claim to qualified immunity and whether or not the deputies held policymaking positions which can be staffed based on political allegiances, the court also dismissed the deputies’ contention that their termination violated their First Amendment right to speak out on a matter of public concern. The court held that merely “liking” a page “is not the kind of substantive statement that has previously warranted constitutional protection.” The decision stirred considerable controversy and debate among constitutional scholars and within the social media industry.

On appeal, the Fourth Circuit overturned the lower court’s holding that Facebook “likes” are too insubstantial to merit First Amendment protection. The court held that “liking” a Facebook page is both pure speech and symbolic speech, and is protected by the First Amendment even with respect to government employees. The court found that the act of “liking” a Facebook page results in publishing a substantive position on a topic. The court reasons that “liking” a political candidate’s campaign page is “the Internet equivalent of displaying



Consumer Attitudes Toward Social Listening

- 32% are unaware that companies are monitoring their social media posts
- 51% do not want companies to engage in social listening
- 43% feel social listening invades their privacy

BUT: 48% say companies should listen in order to improve their products

AND: 58% say companies should respond to online complaints

SOURCE: <http://www.netbase.com/press-release/netbase-survey-reveals-consumers-dont-want-brands-listening-to-social-media-conversations>

a political sign in one’s front yard, which the Supreme Court has held is substantive speech.” As a result, at least within the political context, “likes” enjoy the same strong First Amendment protection that other political speech does.

First Amendment protection for private posts: *Gresham v.*

City of Atlanta. The interplay between social media and the First Amendment was also at issue in the *Gresham* case. In *Gresham*, an Atlanta police officer named Maria Gresham became concerned when a suspect she arrested was taken into a room alone by another officer who turned out to be the suspect’s aunt. The suspect gave some items to his aunt and they

may have spoken. Officer Gresham felt that this constituted an inappropriate interference with her investigation and she aired her concerns by making a Facebook post which was only viewable by her friends. In Atlanta, departmental rules for the conduct of police officers prohibit publicly criticizing other officers. The department received a complaint that Gresham's post had violated these rules and opened an investigation. As a result of that investigation, Gresham was passed over for a promotion. Gresham sued the city, asserting that the department had retaliated against her for engaging in protected First Amendment speech.

The District Court for the Northern District of Georgia found that Gresham's First Amendment interest in making the post was outweighed by the City of Atlanta's interest in maintaining good relations among its police officers. In weighing Gresham's First Amendment interest in making the post, the District Court noted that "the ability of the citizenry to expose public corruption is one of the most important interests safeguarded by the First Amendment." The District Court found that Facebook posts are protected under the First Amendment. It also found, however, that the officer's decision to configure her Facebook post to be viewable only by her friends made "her interest in making the speech . . . less significant than if she had chosen a more public vehicle."

On appeal, the Court of Appeals for the Eleventh Circuit upheld the District Court's decision and expanded on the District Court's reasoning, observing that "the context of Plaintiff's speech is not one calculated to bring an issue of public concern to the attention of persons with authority to make corrections, nor was its context one of bringing the matter to the attention of the public to prompt public discussion to generate pressure for such changes." Because her audience was small and poorly situated to act on the information she shared, the officer's "speech interest is not a strong one." The Court of Appeals agreed with the

District Court that the government has a strong interest in maintaining good relations among police officers, and that this interest outweighed Gresham's weak First Amendment interest in making the post. As a result, the City of Atlanta was found not to have violated Gresham's First Amendment rights by restricting her speech.

The court reasons that "liking" a political candidate's campaign page is "the Internet equivalent of displaying a political sign in one's front yard."

The resulting rule for Gresham and her fellow officers may be somewhat counterintuitive: Atlanta police officers are effectively allowed to criticize one another very privately or very publicly, but the officers risk being disciplined if they criticize another officer in a somewhat public forum. A minor breach of the departmental policy against public criticism is more likely to carry consequences than a major breach is. That being said, the purpose underlying the *Pickering* rule is to ensure that crucial information reaches the public; making a post private undermines that purpose, so it reduces the protection the post receives under the *Pickering* rule.

In any event, with social media becoming more and more integrated into the daily fabric of our lives, one can assume that courts will be struggling with the intersection of free speech rights and social media usage for years to come.

COLLABORATIVE CONSUMPTION – IS IT GOOD TO SHARE?

By [Alistair Maughan](#) and [Susan McLean](#)

Peer-to-peer ("P2P") business models based on the Internet and technology platforms have become increasingly innovative. As such models have proliferated, they frequently result in clashes with regulators or established market competitors using existing laws as a defensive tactic. The legal battles that result illustrate the need for proactive planning and consideration of the likely legal risks during the early structuring phase of any new venture.

Collaborative consumption, or the "sharing economy" as it is also known, refers to the business model that involves individuals sharing their resources with strangers, often enabled by a third-party platform. In recent years, there has been an explosion of these P2P businesses. The more established businesses include online marketplaces for goods and services ([eBay](#), [Taskrabbit](#)) and platforms that provide P2P accommodation ([Airbnb](#), [One Fine Stay](#)), social lending ([Zopa](#)), crowdfunding ([Kickstarter](#)) and car sharing ([BlaBlaCar](#), [Lyft](#), [Uber](#)). But these days, new sharing businesses are appearing at an unprecedented rate; you can now find a sharing platform for almost anything. People are sharing meals, dog kennels, boats, driveways, bicycles, musical instruments — even excess capacity in their rucksacks ([cyclists becoming couriers](#)).

The Internet — and, more specifically, social media platforms and mobile technology — has brought about this economic and cultural shift. Some [commentators](#) are almost evangelical about the potential disruption to traditional economic models that the sharing economy provides, and it's clear that collaborative consumption offers

a compelling proposition for many individuals. It helps people to make money from under-utilized assets and tap into global markets; it gives people the benefits of ownership but with reduced costs and less environmental impact; it helps to empower the under-employed; and it brings strangers together and offers potentially unique experiences. There's clearly both supply and demand, and a very happy set of users for a great many of these new P2P services.

However, not everyone is in favor of the rapid growth of this new business model. Naturally, most of the opposition comes from incumbent businesses or entrenched interests that are threatened by the new competition or those that have genuine concerns about the risk posed by unregulated entrants to the market. Authorities and traditional businesses are challenging sharing economy businesses in a variety of ways, including arguing that the new businesses violate applicable laws, with accommodation providers and car-sharing companies appearing to take brunt of the opposition to date.

BED SURFING

One of the most successful P2P marketplaces, San Francisco-founded [Airbnb](#) is a platform that enables individuals to rent out part or all of their houses or apartments. It currently operates in 192 countries and 40,000 cities. Other accommodation-focused P2P models include [One Fine Stay](#), a London-based platform that allows home owners to rent out empty homes while they are out of town.

Companies such as these have faced opposition from hoteliers and local regulators who [complain](#) that home owners using these platforms have an unfair advantage by not being subject to the same laws as a traditional hotel. City authorities have also cited zoning regulations and other rules governing short-term rentals as obstacles to this burgeoning market. It has been

reported that some residents have been served with [eviction notices](#) by landlords for renting out their apartments in violation of their leases, and some homeowner and neighborhood associations have adopted [rules](#) to restrict this type of short-term rental.

These days, new sharing businesses are appearing at an unprecedented rate; you can now find a sharing platform for almost anything — even for excess capacity in one's rucksack.

These issues are not unique to the United States. Commentators have reported similar resistance — with mixed responses from local or municipal governments — in cities such as Barcelona, [Berlin](#) and Montreal.

It's not particularly surprising that opposition to P2P accommodation platforms would come from existing incumbent traditional operators — after all, that's typical of most new disruptive business models in the early stages before mainstream acceptance. But the approaches taken by P2P opponents illustrate that most regulations were originally devised to apply to full-time commercial providers of goods and services, and apply less well to casual or occasional providers.

This has consequences for regulators, who are likely to have to apply smarter regulatory techniques to affected markets. [Amsterdam](#) is piloting such an approach to accommodation-sharing

platforms, realizing the benefits that a suitably-managed approach to P2P platforms could have on tourism and the local economy.

CAR SHARING

Companies that enable car-sharing services have also faced a barrage of opposition, both from traditional taxi companies and local authorities. In many U.S. cities, operators such as [Lyft](#) and [Uber](#) have faced bans, fines and court battles.

It was [reported](#) in August 2013 that eleven Uber drivers and one Lyft driver were arrested at San Francisco International airport on the basis of unlawful trespassing offenses. In addition, during summer 2013, the Washington, D.C. Taxicab Commission proposed new [restrictions](#) that would prevent Uber and its rivals from operating there. Further, in November 2012, the California Public Utilities Commission (“CPUC”) issued \$20,000 fines against Lyft, SideCar and Uber for “[operating as passenger carriers without evidence of public liability and property damage insurance coverage](#)” and “[engaging employee-drivers without evidence of workers’ compensation insurance](#).”

All three firms appealed these fines, arguing that outdated regulations should not be applied to peer-rental services, and the CPUC allowed the companies to keep operating while it drafted new regulations, which were eventually [issued](#) in July 2013. In August 2013, the Federal Trade Commission intervened and [wrote](#) to the Commissions arguing that the new rules were too restrictive and could stifle innovation. The [CPUC rules](#) (approved on September 19, 2013) require operators to be licensed and meet certain criteria including in terms of background checks, training and insurance. The ridesharing companies will be allowed to operate legally under the jurisdiction of the CPUC, and will now fall under a newly created category called “Transportation Network Company.”

Some operators have structured their businesses in an attempt to avoid at least some of the regulatory obstacles. For example, Lyft does not set a price for a given journey; instead, riders are prompted to give drivers a voluntary “donation.” Lyft receives an administrative fee from each donation. In addition, in its [terms](#), Lyft states that it does not provide transportation services and is not a transportation carrier; rather, it is simply a platform that brings riders and drivers together. In [BlaBlaCar](#)’s model, drivers cannot make a profit, just offset their actual costs, which helps to ensure that drivers are not considered to be traditional taxi drivers, thereby helping them avoid the regulation that applies to the provision of taxi services.

TRADITIONAL PLAYERS EMBRACING THE NEW MODEL

Interestingly, not all traditional players are taking a completely defensive approach. From recent investment decisions, it appears that some companies appreciate that it could make sense for them to work closely with their upstart rivals, rather than oppose them. For example, in 2011, GM Ventures invested \$13 million in RelayRides and, in January 2013, Avis acquired Zipcar, giving Avis a stake in Wheelz, a P2P car rental firm in which Zipcar has invested \$14 million.

The incentive for incumbent operators to embrace P2P models will likely vary by sector. Perhaps it’s no surprise that this is best illustrated in the car rental industry, where there already exists a financial “pull” and a regulatory “push” towards greener and more sustainable models of service provision.

LEGAL AND REGULATORY ISSUES

Lawmakers and businesses around the world are currently grappling with how to interpret existing laws in the context of P2P sharing economy business models and considering whether new regulation is required. For example, the [European Union](#) is preparing an opinion

on collaborative consumption in the light of the growth of P2P businesses there. One hopes that European policy makers focus more on incentivizing public investment in P2P projects via grants or subsidies than on prescriptive regulation of the sector.

Importantly, however, it’s a particular feature of the market for P2P platforms that much of the regulatory activity tends to be at the municipal or local level, rather than national. This tends to make for a less cohesive regulatory picture.

In the meantime, anyone launching a social economy business will need to consider whether and how various thorny legal and regulatory issues will affect both the platform operator and the users of that platform. Often, this may mean tailoring services to anticipate particular legal or regulatory concerns.

- **Consumer protection.** Operators will need to consider the extent to which their platforms comply with applicable consumer protection laws, for example when drafting appropriate terms of use for the platform.
- **Privacy.** Operators will need to address issues of compliance with applicable privacy laws in terms of the processing of the personal data of both users and users’ customers, and prepare appropriate privacy policies and cookie notices.
- **Employment.** Where services are being provided, the operator will need to consider compliance with any applicable employment or recruitment laws, *e.g.*, rules governing employment agencies, worker safety and security, and minimum wage laws.
- **Discrimination.** Operators will need to consider potential discrimination issues, *e.g.*, what are the consequences if a user refuses to loan their car or provide their spare

room on discriminatory grounds, for example due to a person’s race or sexuality? Could the operator attract liability under anti-discrimination laws?

- **Laws relating to payments.** One key to success for a P2P business model is to implement a reliable and effective payment model. But most countries impose restrictions on certain types of payment structures in order to protect consumers’ money. Where payments are made via the P2P platform rather than directly between users, operators will need to address compliance with applicable payment rules, and potentially deal with local [payment services laws](#). Fundamentally, it needs to be clear whose obligation it is to comply with these laws.
- **Taxation.** Operators will need to consider taxation issues that may apply — both in terms of the operator and its users. Some sectors of the economy — hotels, for example — are subject to special tax rates by many cities or tax authorities. In such cases, the relevant authorities can be expected to examine closely — and potentially challenge, or assess municipal, state or local taxes against — P2P models that provide equivalent services. In some places, collection of such taxes can be a joint and several responsibility of the platform operator and its users.
- **Safety and security.** When strangers are being brought together via a platform, security issues will need to be addressed. Most social economy businesses rely on ratings and reciprocal reviews to build accountability and trust among users. However, some platforms also mitigate risks by carrying out background and/or credit checks on users. Airbnb also takes a practical approach, employing a full-time [Trust & Safety](#) team to provide extra assurance for its users.

- **Liability.** One of the key questions to be considered is who is legally liable if something goes wrong. Could the platform attract liability if a hired car crashes or a host's apartment is damaged?
- **Insurance.** Responsibility for insurance is also a key consideration. The issue of insurance for car-sharing ventures made headlines in April 2013 when it was reported that a Boston resident had crashed a car that he had borrowed via RelayRides. The driver was killed in the collision and four other people were seriously injured. RelayRides' liability insurance was capped at \$1 million, but the claims potentially threaten to exceed that amount. Given these types of risks, some insurance companies are refusing to provide insurance coverage if policyholders engage in P2P sharing. Three U.S. states (California, Oregon and Washington) have passed laws relating to car sharing, placing liability squarely on the shoulders of the car-sharing service and its insurers.
- **Industry-specific law and regulation.** Companies will need to consider issues of compliance with any sector-specific laws, whether existing laws or new regulations that are specifically introduced to deal with their business model (such as crowd-funding rules under the JOBS Act in the United States, and P2P lending rules to be introduced shortly in the United Kingdom). As noted above, some social economy businesses have already experienced legal challenges from regulators, and as collaborative consumption becomes even more widely adopted, regulatory scrutiny is likely to increase. Accordingly, rather than resist regulation, the best approach for sharing economy businesses may be to create trade associations for their sector and/or engage early on with lawmakers and regulators in order to design appropriate, smarter

policies and frameworks for their industry.

CONCLUSION

Erasmus said, "There is no joy in possession without sharing." Thanks to collaborative consumption, millions of strangers are now experiencing both the joy — and the financial benefits — of sharing their resources. However, the legal challenges will need to be carefully navigated in order for the sharing economy to move from being merely disruptive to become a firmly established business model.

POTENTIAL LIMITATIONS PLACED ON UNILATERAL RIGHT TO MODIFY TERMS OF USE

By Jacob Michael Kaufman

Contractual provisions giving a website operator the unilateral right to change its end user terms of service are ubiquitous and appear in the online terms of many major social media sites and other websites, including Facebook, Twitter, Instagram and Google. Although amendments to terms of service quite often cause consumers to complain, litigation regarding such changes is relatively rare. A recent decision from the U.S. District Court in the Northern District of Ohio, however, challenges the enforceability of unilateral amendments to online terms of service in at least some circumstances.

In *Discount Drug Mart, Inc. v. Devos, Ltd. d/b/a Guaranteed Returns*, Discount Drug Mart, a distributor of pharmaceuticals, sued Guaranteed Returns, a company that processes pharmaceutical product returns, for Guaranteed Returns' failure to remit credits due under a written distribution agreement between the parties. Guaranteed Returns pointed to the forum selection clause on its website, which

it argued required the parties to bring suit in either Nassau or Suffolk County in the State of New York. This provision appeared in Guaranteed Returns' online "standard terms and conditions," which Guaranteed Returns claimed were incorporated into the parties' written distribution agreement.

The court held otherwise, citing the Sixth Circuit case *Int'l Ass'n of Machinists and Aerospace Workers v. ISP Chemicals, Inc.* and stating that "[i]ncorporation by reference is proper where the underlying contract makes clear reference to a separate document, the identity of the separate document may be ascertained, and incorporation of the document will not result in surprise or hardship." The court also pointed out that Guaranteed Returns' purported right to change its standard terms and conditions unilaterally could result in Discount Drug Mart being subject to surprise or hardship. Further, the court noted that there was no evidence that the forum selection clause had been included in the standard terms and conditions at the time the distribution agreement was signed (and Guaranteed Returns did nothing to try to prove this fact). Thus, the court concluded that the standard terms and conditions were not properly incorporated into the distribution agreement (although the court ended up finding in favor of Guaranteed Returns on other grounds).

It is difficult to say what, if any, precedential force *Discount Drug Mart* will have. Putting aside the facts that the case was brought in the Northern District of Ohio and was ultimately dismissed on grounds unrelated to this holding, the underlying background of the case was nuanced. First, although the court stated *in dicta* that "one party to a contract may not modify an agreement without the assent of the other party," a statement that could be interpreted to mean that unilateral amendment of contracts is never permitted, the holding itself was limited to situations in which terms and conditions are incorporated by reference. That said, even this limited

holding may be relevant to many website operators in the social media world, as the larger social media sites often use a network of contracts that reference each other (for example, Facebook’s “Platform Policies” requires developers to agree to the company’s “Statement of Rights and Responsibilities,” which are “requirements for anybody who uses Facebook” and which can be unilaterally modified by Facebook).

Second, the *Discount Drug Mart* court did not elaborate on the “surprise or hardship” standard, so it is possible that unilateral changes to end user terms would be upheld if the website operator gave proper notice to its end users of such changes in order to avoid causing surprise or hardship. The leading social media platforms currently have different approaches to providing notice of changes to their online terms of use. For example, Facebook provides seven days’ notice (although “notice” here includes posting on Facebook’s site governance page); Twitter will notify users of changes to its terms of service via an “@Twitter” update or through email (but only for changes that Twitter deems to be material in its sole discretion); and Instagram notifies users of its changes to its terms of use by posting them on Instagram. A court could find that notification of changes using one or more of these methods is sufficient to avoid subjecting an end user to surprise or hardship.

Finally, the court seemed to give weight to the lack of any evidence that the forum selection clause was included in Guaranteed Returns’ standard terms and conditions at the time that the parties entered into the distribution agreement. Today, however, most Internet service providers include “last modified” dates in their terms of use. Recording version dates and keeping copies of older terms of use could help a website operator show that a particular provision existed in terms of use at the time that the parties entered into an agreement referencing such terms (although these practices could also provide evidence to the contrary).

The case suggests that if a company includes language allowing it to make unilateral changes to its terms by simply posting the revised terms on its website, those terms could be deemed invalid.

Discount Drug Mart is not the first decision to challenge a company’s right to unilaterally modify its online terms and conditions. In the 2007 case *Douglas v. Talk America*, the Ninth Circuit Court of Appeals held that Talk America could not enforce an arbitration clause against an individual who had initially accepted the applicable terms of service prior to Talk America’s unilateral addition of the arbitration clause. Although Talk America posted the amended terms online, the court noted that the individual’s assent to the new terms could only be inferred “after [the individual] received proper notice of the proposed changes.” *Discount Drug Mart* seems consistent with this decision to the extent that the case suggests that failure to provide adequate notice to end users of changes to online terms may invalidate such changes.

A decision in the Northern District in the U.S. District Court of Texas in 2009, *Harris v. Blockbuster Inc.*, went further than the *Douglas* court by holding an arbitration clause in Blockbuster’s online terms of use rendered the terms of use illusory and unenforceable. The court’s holding was based on the fact that Blockbuster could, in theory,

unilaterally modify the arbitration provisions and apply those modified provisions to earlier disputes. *Harris* cited the Fifth Circuit case, *Morrison v. Amway Corp.*, in which the court had held an arbitration clause in online terms of use to be illusory under Texas law when defendant Amway attempted to apply arbitration terms that had been modified after the plaintiff had agreed to Amway’s standard terms. Although limited to the Northern District of Texas (for now), the implications of *Harris* could be troubling to online service providers, as the case suggests that if a company includes language allowing it to make unilateral changes to its terms by simply posting the revised terms on its website, those terms could be deemed invalid. In fact, at least one legal scholar has suggested that companies should not include such language in their online terms. For more on *Harris*, see our client alert [here](#).

Discount Drug Mart does not necessarily provide any clear guidelines that online service providers must follow for their online terms to be valid and enforceable. Because the court based its holdings on specific factual circumstances and provided little insight into its reasoning, it is unclear at this point whether other courts will follow this opinion and impose limitations on companies’ rights to unilaterally change their online terms of service under different circumstances. However, given the legal precedent on the subject, it will likely behoove companies that incorporate their online terms into other documents to consider re-evaluating their amendment and notification practices to minimize any chance of subjecting end users to “surprise or hardship.”

A WARNING FOR WEBSITES ALLOWING DATA COLLECTION FOR ONLINE BEHAVIORAL ADVERTISING

By Reed Freeman, Adam Fleisher and Patrick Bernhardt

The Better Business Bureau's Online Interest-Based Advertising Accountability Program ("the Accountability Program") issued its first ever compliance warning on October 14, a move that is intended to clarify the obligations of websites where data are gathered for Online Behavioral Advertising ("OBA") purposes. The result is that operators of such websites are now expected to ensure that consumers receive "enhanced notice" under the the Digital Advertising Alliance ("DAA") Self-Regulatory Principles for Online Behavioral Advertising (the "Principles"), and cannot simply rely in all instances on third parties, such as ad networks, to bring the websites into compliance with the Principles by displaying such notice within OBA ads appearing on the operators' websites. Failure to meet this requirement can result in an enforcement action by the Accountability Program beginning on January 1, 2014.

The Accountability Program's compliance warning concludes its investigation into whether a number of websites were in compliance with the Principles as they relate to first-party obligations (that is, obligations for websites with whom the consumer is interacting, as opposed to ad networks and others, which are generally referred to as "third parties" in the Principles). According to the Accountability Program, a significant minority of website operators otherwise in compliance with the Principles were not providing "enhanced notice" on every web page where data is *collected* for interest-based advertising by third

parties. (Although the warning focuses on compliance in the context of third-party collection of data for OBA, the requirements also apply in cases where a website operator collects data on its own webpage and transfers the data to a third party for use for OBA purposes on non-affiliate webpages.) This type of notice — in addition to the notice regarding delivery of interest-based advertisements that is commonly provided within the OBA ads themselves — is, according to the Accountability Program, also required by the OBA Principles, at least on those pages where data are collected for OBA purposes but where no such OBA ads bearing the enhanced notice appear.

According to the Accountability Program, many companies are "genuinely confused" about their first-party notice obligations under the Principles. Hence the compliance warning, rather than a set of case decisions, which explains that the Transparency Principle of the OBA Principles requires websites to provide notice outside of their privacy policies whenever third parties collect a consumer's browsing activity for OBA purposes. As the compliance warning puts it, the Transparency Principle "shines a light on interest-based advertising whenever and wherever it is occurring online." This includes the *collection* of information regarding browsing activities by third parties for their use in interest-based advertising — not just the actual *delivery* of interest-based ads.

Simply put, this compliance warning makes clear that under the DAA's OBA Principles, first parties have a responsibility to make sure that consumers are aware that OBA activities are occurring on the website, whether by third parties displaying it in or around OBA ads on the website, or on pages where OBA ads are not delivered, by the first party itself. Since the Accountability Program will start enforcing this requirement on January 1, 2014, websites that allow third parties to collect information for OBA purposes will need to have in place a separate notice mechanism.

HOW TO COMPLY

First parties can comply with this requirement by:

(1) using a "clear, meaningful, and prominent link" on the website itself (the "enhanced notice link" — this is separate from the privacy policy link, and can be the AdChoices Icon or a text link); that

(2) takes the user to the first party's disclosure of OBA activity, such as the specific portion of the first party's website that addresses OBA activity; which itself must either:

(a) point to an industry-developed Web page such as the DAA's Consumer Choice Page (e.g., www.aboutads.info/choices); or

(b) individually list all third parties engaged in OBA on the website, with links to the choice mechanisms regarding the collection and use of data for OBA for each applicable third party. (The new warning cautions that any website operator that chooses to individually list each third party collecting data for OBA on its website must provide an accurate, up-to-date and comprehensive list, which in practice requires sufficient technical and/or contractual safeguards to prevent unauthorized third parties from engaging in OBA collection.) Website operators that provide an individual list need to make sure that it is accurate and up-to-date, and that there are no unauthorized third parties engaging in OBA data their websites.

Website operators are now on notice that the DAA's transparency and choice principles for OBA require more than enhanced notice for the *delivery* of OBA advertisements. According to the compliance warning, the only way a website operator could be in full compliance without providing the information described above is if OBA ads bearing in-ad notice are served on every page of the website where third parties are also *collecting* data for OBA — and, even then, those in-ad notices would have to provide information on *all* third parties collecting data on the website.

PRACTISING LAW INSTITUTE'S SOCIAL MEDIA 2014: ADDRESSING CORPORATE RISKS

Did you know that Facebook now has *well over one billion monthly active users*? (By contrast, the entire population of the United States is 314 million people.) Or that Facebook accounts for over ten percent of all U.S. web traffic? And that *over 300 million photographs* are posted to Facebook each day? Or that Twitter users are expected to send over 146 billion tweets during 2013? And that *over six billion hours of video* are viewed each month on YouTube, almost an hour for every person on Earth?

Facebook, Foursquare, Google+, LinkedIn, Pinterest, Tumblr, Twitter, YouTube and other social media sites are transforming not only the daily lives of consumers, but also how companies interact with consumers. Indeed, even the largest, most conservative blue-chip corporations have begun to embrace social media; one study revealed that, of the Fortune Global 100, 82% had Twitter accounts; 74% had a presence on Facebook; and 79% had a YouTube channel; these numbers will only increase over time. Many marketing professionals view social media as the single greatest marketing tool to have emerged in this century.

However, along with the exciting new marketing opportunities presented by social media comes challenging new legal issues. In seeking to capitalize on the social media gold rush, is your company taking the time to identify and address the attendant legal risks? The good news is that, merely by undertaking simple, low-cost precautions,

companies seeking to use social media can significantly reduce their potential liability exposure.

Please join us as leading practitioners and industry experts explore the cutting-edge legal concerns emerging from social media, and provide practical solutions and real-world insights to assist you in tackling these concerns.

What you will learn

- Social media: how it works, and why it is transforming the business world
- Drafting and updating social media policies
- User-generated content and related IP concerns
- Ensuring protection under the CDA's Safe Harbor
- Legal issues in connection with online data harvesting
- Online marketing: new opportunities, new risks
- Privacy law considerations
- Practical tips for handling real-world issues

This conference is being held in San Francisco on February 10, 2014 and in New York City on February 26, 2014; the February 10th event will be webcasted. Socially Aware co-editor John Delaney will serve as conference chair and representatives from top social media companies will be presenting at the event. For more information or to register, please visit PLI's website at www.pli.edu/content.

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 in many areas. Our clients include some of the largest financial institutions, Fortune 100 companies, investment banks and technology and life science companies. Our clients count on us for innovative and business-minded solutions. Our commitment to serving client needs has resulted in enduring relationships and a record of high achievement. For the last 10 years, we've been included on *The American Lawyer's* A-List. *Fortune* named us one of the "100 Best Companies to Work For." Our lawyers share a commitment to achieving results for our clients, while preserving the differences that make us stronger.

Because of the generality of this newsletter, the information provided herein may not be applicable in all situations and should not be acted upon without specific legal advice based on particular situations. The views expressed herein shall not be attributed to Morrison & Foerster, its attorneys or its clients.

©2013 Morrison & Foerster LLP, mofo.com