Volume 8, Issue 1, January/February 2017

SOCIALLY AWARE

THE SOCIAL MEDIA LAW UPDATE

2011 BEST LAW FIRM NEWSLETTER

IN THIS ISSUE

EDITORS

John F. Delaney
Aaron P. Rubin

CONTRIBUTORS

John F. Delaney
Aaron Rubin
Adam Fleisher
Holger Andreas Kastler
Susan McLean
Andrew Serwin
Leanne Ta
Nathan Taylor
Miriam Wugmeister

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 examine a spate of court decisions that appear to rein in the historically broad scope of the Communications Decency Act's Section 230 safe harbor for website operators; we outline ten steps companies can take to be better prepared for a security breach incident; we describe the implications of the Second Circuit's recent opinion in *Microsoft v. United States* regarding the U.S. government's efforts to require Microsoft to produce email messages stored outside the country; we explore the EU's draft regulation prohibiting geo-blocking; and we take a look at UK Consumer Protection regulators' efforts to combat undisclosed endorsements on social media.

All this—plus an infographic highlighting the most popular social-media-post topics in 2016.

MOST POPULAR POST TOPICS IN 2016

MOST POPULAR[1]

1. #Rio2016
2. #Election2016
3. #PokemonGo
4. #Euro2016
5. #Oscars
6. #Brexit
7. #BlackLivesMatter
8. #Trump
9. #RIP
10. #GameofThrones

MOST DISCUSSED (GLOBAL)[2]

1. U.S. Presidential Election
2. Brazilian Politics
3. Pokemon Go
4. Black Lives Matter
5. Rodrigo Duterte & Philippine Presidential Election
6. Olympics
7. Brexit
8. Super Bowl
9. David Bowie
10. Muhammad Ali

MOST FOLLOWED PERSON[3]

Selena Gomez

MOST-LIKED PHOTO[3]

A Selena Gomez post sponsored by Coca-Cola

MOST FOLLOWED BRANDS[3]

1. National Geographic
2. Nike
3. Victoria's Secret

MOST POPULAR HASHTAG[4]

#love

SOURCES

1. http://money.cnn.com/2016/12/06/technology/twitter-top-events-hashtags-2016/
2. http://newsroom.fb.com/news/2016/12/facebook-2016-year-in-review/
3. https://later.com/blog/instagram-year-in-review-2016/
4. http://www.cnn.com/2016/12/02/us/instagram-year-in-review-trnd/

THE DECLINE AND FALL OF THE SECTION 230 SAFE HARBOR?

By Leanne Ta and Aaron Rubin

2016 was a tough year for a lot of reasons, most of which are outside the scope of this blog (though if you'd like to hear our thoughts about Bowie, Prince or Leonard Cohen, feel free to drop us a line). But one possible victim of this *annus horribilis* is well within the ambit of Socially Aware: Section 230 of the Communications Decency Act (CDA).

Often hailed as the law that gave us the modern Internet, CDA Section 230 provides immunity against liability for website operators for certain claims arising from third-party or user-generated content. The Electronic Frontier Foundation has called Section 230 "the most important law protecting Internet speech," and companies including Google, Yelp and Facebook have benefited from the protections offered by the law, which was enacted 20 years ago.

But it's not all sunshine and roses for Internet publishers and Section 230, particularly over the past 18 months. Plaintiffs are constantly looking for chinks in Section 230's armor and, in an unusually large number of recent cases, courts have held that Section 230 did not apply, raising the question of whether the historical trend towards broadening the scope of Section 230 immunity may now be reversing. This article provides an overview of recent cases that seem to narrow the scope of Section 230.

THE "PUBLISHER OR SPEAKER" REQUIREMENT

CDA Section 230(c)(1) states that "no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." Plaintiffs sometimes argue that Section 230 does not apply because the claims they are asserting do not treat the defendant as a publisher or speaker. This has not always been a successful argument, but it has prevailed in several recent cases.

Doe #14 vs. Internet Brands involved a website called Model Mayhem, which is designed to match models with prospective gigs. In 2012, a Jane Doe plaintiff sued Internet Brands, the parent company of Model Mayhem, alleging that the site's operators were negligent in notifying its users of the risk that rapists were using the website to find victims. Consequently, Doe argued, she was drugged and raped by two assailants who had used the website to lure her to a fake audition.

One of the most commonly exploited plaintiff's arguments against the section 230 defense is that the statutory immunity does not apply if the defendant itself developed or contributed to the relevant material.

The plaintiff argued that Section 230 did not apply because a "failure to warn" claim did not depend on Model Mayhem being the publisher or speaker of content provided by another person. The Ninth Circuit bought the plaintiff's argument and overturned the district court's earlier dismissal of the case, which had been based on Section 230 immunity.

In his opinion, Judge Clifton explained that Jane Doe did not seek to hold Internet Brands liable as a publisher or speaker of content posted by a user on the website, or for its failure to remove content posted on the website. Instead, she sought to hold Internet Brands liable for failing to warn her about information it obtained from an outside source about how third parties targeted victims through the website. This duty to warn would "not require Internet Brands to remove any user content or otherwise affect how it publishes or monitors such content." Since the claim did not treat Internet Brands as a publisher or speaker, the court ruled that Section 230 did not apply.

Some commentators have criticized this ruling, arguing that imposing an obligation on website operators to warn about potentially harmful users is impractical and contrary to the principles of Section 230 and of many prior cases and will cause websites to self-censor and over-censor.

A similar argument worked—to an extent—in *Darnaa v. Google*, a Northern District of California case that involved YouTube's removal of the plaintiff's music video based on YouTube's belief that the plaintiff had artificially inflated view counts. The plaintiff sued for breach of the covenant of good faith and fair dealing, interference with prospective economic advantage and defamation. She sought damages and an injunction to prevent YouTube from removing the video or changing the video's URL.

The district court held that Section 230(c)(1) preempted the plaintiff's interference claim, but not her good faith and fair dealing claim. The court explained that the latter claim sought to hold YouTube liable for breach of its good faith contractual obligation to the plaintiff, rather than in its capacity as a publisher; as such, Section 230 did not shield YouTube against this claim.

In a similar vein, a California Court of Appeal refused to apply the Section 230 safe harbor in a case involving Yelp, which we recently wrote about. In *Hassell v. Bird*, the plaintiff, an attorney, sued a former client for defamation regarding three negative reviews that the plaintiff claimed the defendant had published on Yelp.com under different usernames. When the defendant failed to appear, the court issued an order granting the plaintiff's requested damages and injunctive relief. The court also entered a default judgment ordering Yelp to remove the offending posts. Yelp challenged the order on Section 230 grounds, among others, but the court held that Section 230 did not apply. It reasoned that Yelp was not itself being sued for defamation, so it did not face liability as a speaker or publisher of third-party speech.

Likewise, the Northern District of California court in *Airbnb v. City and County of San Francisco* denied Airbnb's request for a preliminary injunction barring enforcement of a San Francisco ordinance that makes it a misdemeanor to provide booking services for unregistered rental units. Airbnb argued that such an ordinance would conflict with Section 230, which contains an express preemption clause stating that no liability may be imposed under any state or local law that is inconsistent with Section 230.

The decision turned on whether the ordinance "inherently requires the court to treat [Airbnb] as the 'publisher or speaker' of content provided by another." Airbnb argued that the threat of criminal penalty for providing booking services for unregistered rental units would require that the company actively monitor and police listings by third parties to verify registration, which would be tantamount to "treating it as a publisher" because that would involve traditional publisher functions of reviewing, editing and selecting content to publish.

But the court held that the ordinance did not treat Airbnb as the publisher or speaker of the rental listings because the ordinance applies only to providing and collecting fees for booking services in connection with an unregistered unit and does not regulate what can and cannot be published. Therefore, the court denied the request for preliminary injunction.

SECTION 230'S APPLICATION TO "PROVIDERS AND USERS"

Plaintiffs sometimes argue along with the "publisher or speaker" argument

that Section 230 does not apply where the defendant does not fall within the category of "providers and users of an interactive computer service," as required under Section 230(c)(1). This argument worked for the plaintiff in *Maxfield v. Maxfield*, a Connecticut state court case.

In *Maxfield*, the plaintiff sued his ex-wife for defamation, claiming that she forwarded screenshots of defamatory tweets about him to his current wife. The ex-wife defended on Section 230 grounds, based on the fact that she forwarded third-party tweets but did not write the tweets herself. The court, however, found that she was not covered by Section 230 immunity because she "merely transmitted" the defamatory messages. The opinion states: "Ms. Maxfield does not operate a website and plainly is not 'a provider of an interactive computer service.' While she might, on occasion, be considered a 'user of an interactive computer service,' she did not do so in the behavior alleged in the complaint." Therefore, the court rejected the defendant's Section 230 defense.

It is worth noting that the *Maxfield* decision runs contrary to several prior cases in which courts have held that forwarding defamatory emails would, in fact, be covered by Section 230.

DEFENDANTS AS CONTENT DEVELOPERS

One of the most commonly exploited plaintiff's arguments against Section 230 defenses is that the statutory immunity does not apply if the defendant itself developed or contributed to the relevant material. In other words, the relevant material is not "information provided by *another* information content provider" and therefore falls outside of the scope of Section 230. Courts have historically been fairly strict about applying this exception, and have consistently held that editing, selecting and commenting on third-party content does not take a defendant out of Section 230 immunity. However, recent cases seem to blur the line between what it means to "develop" content and to exercise editorial functions.

In *Diamond Ranch Academy v. Filer*, the plaintiff, who ran a residential youth treatment facility, sued the defendant, who ran a website that contained critical descriptions of the plaintiff's facility, for defamation. The critical comments were included in a portion of the website that, according to the defendant, contained third-party complaints about the plaintiff. The defendant asserted a Section 230 defense, arguing that she had merely selected and summarized third-party material to make it more digestible for readers.

However, the court did not find this argument persuasive. In its decision, the court pointed out that the defendant's posts "do not lead a person to believe that she is quoting a third party. Rather, [she] has adopted the statements of others and used them to create her comments on the website." The court implied that the lack of quotation marks or other signals that the comments were created by third parties supported the inference that the defendant had "adopted" the statements. The court also noted that she had "elicited" the third-party comments through surveys that she had conducted. Since it treated the defendant as the author of the allegedly defamatory statements, the court held that she was not entitled to protection under Section 230 for those statements.

In a more recent ruling, the Seventh Circuit in *Huon v. Denton* similarly refused to immunize the defendant from liability for an allegedly defamatory comment posted on its website. The case involved a comment to a story published on Jezebel, a property owned by Gawker, that called the plaintiff a "rapist." The plaintiff argued that Section 230 was inapplicable because "Gawker's comments forum was not a mere passive conduit for disseminating defamatory statements." Rather, the plaintiff claimed, Gawker itself was an information content provider because it "encouraged and invited" users to defame the plaintiff, through "urging the most defamation-prone commenters to post more comments and continue to escalate the dialogue," editing and shaping the content of the comments and selecting each comment for publication.

Many prior cases have held that engaging in editorial activities such as these does not turn a website operator into a content developer for purposes of Section 230. But the court in *Huon* sidesteps these arguments, stating that "we need not wade into that debate" because the plaintiff had also alleged that Gawker employees may have anonymously authored comments to increase traffic to the website. Despite the fact that, as one commentator noted, there was no allegation that Gawker employees had written the specific allegedly defamatory comment at issue, the court held that these allegations of anonymous authorship by Gawker employees were sufficient to survive Gawker's motion to dismiss.

AVOIDANCE OF SECTION 230(C)(2) ON TECHNICALITIES

So far, this article has focused primarily on CDA Section 230(c)(1), which tends to see more action in the courts than its counterpart provision, CDA Section 230(c)(2). But there have also been recent cases that narrow the scope of Section 230(c)(2).

Section 230(c)(2) states that no provider or user of an interactive computer service will be liable for its filtering decisions. Specifically, Section 230(c)(2)(A) protects website operators from liability for "any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected." Arguably, plaintiffs have reasoned, Section 230(c)(2) does not apply to filtering decisions that are based on other objections.

In *Song Fi v. Google Inc.*, another case involving the removal of a video for allegedly inflated view counts that we previously covered, the plaintiff asserted claims for, among other things, breach of contract and breach of the implied covenant of good faith and fair dealing. The defendant, YouTube, raised a defense under Section 230(c)(2). However, the court interpreted the provision narrowly and found that although videos with inflated view counts could be a problem for YouTube, they are not "otherwise objectionable" within the meaning of Section 230(c)(2)(A).

As we wrote previously, the court concluded that, in light of the CDA's history and purpose, the phrase "otherwise objectionable" relates to "potentially offensive material, not simply any materials undesirable to a content provider or user." Further, the requirement that the service provider subjectively finds the blocked or screened material objectionable "does not mean anything or everything YouTube finds subjectively objectionable is within the scope of Section 230(c)." The court did not believe that YouTube's removal of the video was "the kind of self-regulatory editing and screening that Congress intended to immunize in adopting Section 230(c)." Therefore, the court held that YouTube's removal of videos with inflated view counts fell outside of the protections offered by Section 230(c)(2).

LOOKING AHEAD

So where do these cases leave us? Unfortunately for website operators, and happily for plaintiffs, there seems to be a trend developing toward reining in the historically broad scope of Section 230 immunity. Of course, Section 230 still provides robust protection in many cases, and we have also seen a few recent victories for defendants asserting Section 230 defenses. Whatever happens, we will continue to monitor and provide updates on Section 230 as we enter the new year.

PREPARING FOR A DATA SECURITY BREACH: TEN IMPORTANT STEPS TO TAKE

By Miriam Wugmeister, Andrew Serwin and Nathan Taylor

Is your company prepared to respond to a data security breach? For many companies, even reading this question causes some anxiety. However, being prepared for what seems like the inevitable—a security breach—can be the difference between successfully navigating the event or not. While we still hear some companies say *"That would never happen to our company!"* a significant breach can happen to any company.

In light of this and the close scrutiny that the high-profile breaches reported over the past year have received, many companies have taken the opportunity to consider their preparedness and ability to respond quickly and decisively to such an incident. We have prepared for our readers who are in-house attorneys or privacy officers the following checklist highlighting some steps that companies may consider taking so that they can be better prepared in the event that a significant breach incident occurs.

1. MAKE FRIENDS WITH YOUR IT/IS DEPARTMENT.

It is important to be familiar with your company's risk tolerance and approach to information security in order to develop an understanding of your company's security posture. The time to explore these issues isn't *after* a breach has happened, so ask your colleagues in your company's information technology or information security departments the basic questions (e.g., What's DLP?) and the tough questions (e.g., Why haven't we addressed the data security concerns raised in last year's audit?). You would rather learn, for example, that your company does not encrypt its laptops before one is stolen.

2. HAVE A PLAN.

Many companies have an incident response plan. If your company does, dust it off. Does it need to be updated based on the current breach environment? Would it actually be helpful in responding to a high-profile nationwide data security breach? Does it have a list of key contacts and contact information? Also, make sure you have a copy printed out in case the breach impacts your company's electronic system. If you don't have a plan, draft one and implement it.

3. PRACTICE.

Although practice may not make perfect when it comes to data breach response, you do not want your response team working together for the first time in the middle of an actual high-stress incident. Gather your response team and relevant stakeholders and conduct a "fire drill" or "breach tabletop exercise" (and consider bringing your outside counsel). This will be invaluable training and an investment in your company's preparedness.

4. DECISIONS, DECISIONS, DECISIONS.

Someone has to make the tough calls. A high-profile breach incident presents a series of tough calls (e.g., when will you go public, how will you respond to the media, will you offer credit monitoring and so forth). We continue to hear of incidents where there are competing views within a company about the "right" decision, and incidents where difficult decisions have to be made based on limited facts. You should give thought to who within your organization will be responsible for making the tough calls and making sure the key decision-makers understand the broader issues that have to be considered.

5. KNOW THE LAW.

In the United States, notice of breach incidents is driven by federal

and state law. There are federal breach requirements (e.g., the Gramm-Leach-Bliley Act), and there are state requirements in 51 states and jurisdictions. Needless to say, notice in a nationwide incident can be complicated. And the laws have been rapidly changing over the last several years. Someone in your company should be committed to staying abreast of the current landscape of breach-related requirements (e.g., requirements for the content of consumer notices and requirements to notify state regulators). In addition, breaches that affect individuals outside the United States are even more complicated. Be aware that the number of jurisdictions with breach-notification obligations is growing, and in many instances a "breach" includes the unauthorized disclosure of any type of personal information.

6. GO OUTSIDE.

Outside counsel who have a deep practice in this area will have worked on countless incidents both large and small and can advise on how other companies respond to similar incidents and how regulators have reacted. This is invaluable insight when the tough calls have to be made (see item 4 above).

7. ENGAGE VENDORS.

In a significant breach incident, a company's resources can be stretched thin. Many companies would not have the capability to produce and mail 500,000 breach letters in just a few days. Similarly, many companies are not prepared to handle dramatically increased call center volumes after an incident becomes public. There are a wide variety of vendors that can help companies respond to a breach incident, including forensic investigators, crisis communication experts and mail houses, to name a few. Consider your company's capabilities and engage vendors *before* an incident occurs.

8. IN CASE OF EMERGENCY, CALL.

The list of individuals and entities that may need to be contacted in case of a significant breach at your company may be longer than you think. For example, you may need to contact members of your response team, members of senior management, your merchant acquirer, payment card networks, a wide variety of vendors, the press, your regulators, outside counsel and others. While a comprehensive contact list may seem simple, it can reduce stress in the heat of the moment if you have one (see item 2 above).

Be aware that the number of jurisdictions with breach-notification obligations is growing, and in many instances a "breach" includes the unauthorized disclosure of any type of personal information.

9. CONSIDER COVERAGE.

Cyber insurance is one of the fastest growing areas of insurance today. It's quite possible that your company already has a policy that would provide at least some coverage in the case of a data security breach. If so, the policy should be reviewed to get a sense of the breadth of the coverage and to determine whether such coverage is appropriate for your company's needs. If your company does not have a policy, you can consider the costs and benefits of obtaining coverage. This is a risk-based decision, but one that of course needs to be thought about before a breach occurs.

10. DON'T DELAY.

Although you can't control whether a breach occurs, you can control how your company responds. Many companies will find that there is more that they can do to prepare for a potential breach event. In light of the public, regulatory and internal scrutiny that a high-profile breach brings, you should not delay in considering your company's preparedness to respond to such an event.

CONCLUDING THOUGHTS

Unfortunately, data security breaches have become as inevitable as death and taxes; accordingly, no company can afford to be unprepared for a breach incident when it occurs. Although our pre-breach checklist above isn't intended to be exhaustive, it should provide a helpful starting point for companies in thinking about the unthinkable.

SECOND CIRCUIT: EMAIL STORED OUTSIDE THE UNITED STATES MIGHT BE BEYOND GOVERNMENT'S REACH

By Andrew Serwin and Adam Fleisher

As a result of the Second Circuit's recent opinion in *Microsoft v. United States*, the U.S. government likely can no longer use warrants issued pursuant to the Stored Communications Act (SCA) to compel U.S.-based companies to produce communications, such as emails, that are stored in a physical location outside of the United States—at least for now. Instead, the government will likely need to rely on Mutual Legal Assistance Treaties, which provide a framework for states to, among other things, provide assistance to one another to obtain and execute search warrants in their respective jurisdictions.

Nevertheless, it is likely that the U.S. government will seek an alternative, which could include appealing the case to the Second Circuit en banc or pursuing legislation in Congress to amend and update the SCA in light of new digital realities.

BACKGROUND ON THE SCA AND THE MICROSOFT DISPUTE

The SCA, which limits service providers' disclosure of the user data they store, provides that a service provider may disclose to the government certain information, such as the stored contents of a customer's emails, only if the government first obtains a warrant requiring the disclosure. *Microsoft v. United States* arose out of Microsoft's dispute over the scope of one such warrant, which sought information about an email account that Microsoft determined was hosted in Dublin.

Microsoft moved to quash the warrant with respect to the actual emails in the account on the grounds that the SCA does not authorize a search and seizure outside of the territory of the United States, which is where the emails were stored.

SUMMARY OF THE SECOND CIRCUIT RULING

The Second Circuit reached its decision by answering three questions:

- **What is a warrant under the SCA?** Is it like a quasi-subpoena that would require a company to produce documents or information under the company's control, *regardless* of where the information may be physically located? Or is it truly a warrant that only provides the government the right to conduct a search or obtain documents or information based on the statutory authority underlying the warrant (i.e., the scope of the SCA itself)?
- **What is the scope of the SCA?** If the scope of the warrant is limited to the scope of the SCA, then the next vitally important question is whether the authority of the SCA is limited to the United States or extends extraterritorially. If the SCA does not extend beyond the borders of the United States, neither would the warrant.

The Second Circuit agreed that the warrant was not enforceable outside of the boundaries of the United States, and that because the emails were stored outside of the United States and would need to be accessed outside of the United States, they could not be extracted under the SCA.

- **What action was required pursuant to the warrant, and did that action take place in the United States?** Even if the court found that the SCA and, therefore, the warrant were confined to the territory of the United States, the court still had to address *where* the seizure of the emails would occur. Microsoft had the technical ability to access the emails from the United States, but argued that the emails themselves were located in Dublin, a foreign jurisdiction.

The Second Circuit agreed with Microsoft and found that the warrant was not enforceable outside of the boundaries of the United States, and that because the emails were stored outside of the United States and would need to be accessed outside of the United States, they could not be extracted from Dublin under the SCA.

THE SCOPE OF AN SCA WARRANT

First, Microsoft argued that the warrant contemplated by the SCA is not a "hybrid" of a warrant and a subpoena but, rather, purely a warrant. This distinction mattered because a subpoena may require the production of communications stored overseas, while a warrant may be more limited. A subpoena can be served on a company and call for materials within the company's possession and control, *regardless* of where the information is physically located. Citing the Second Circuit's 1983 decision in *Marc Rich & Co., A.G. v. United States*, the court explained that relevant precedent provides that "a defendant subject to the personal jurisdiction of a subpoena-issuing grand jury could not 'resist the production of [subpoenaed] documents on the ground that the documents are located abroad.'"

A warrant, however, only provides the government with a right to conduct a search or obtain documents or information. That right cannot extend beyond the scope of the statutory authority forming the basis for the warrant. And, because it was authorized under the SCA, if the warrant were truly a warrant, it would only encompass the authority to obtain information covered by the SCA (as opposed to all information within Microsoft's possession).

The district court, in denying Microsoft's motion to quash, had reasoned that the SCA warrant was like a subpoena because, in the words of the Second Circuit, "it is executed by a service provider rather than a government law enforcement agent, and because it does not require the presence of an agent during its execution." In other words, the government simply served the warrant to Microsoft, and Microsoft then searched for and provided relevant materials to the government (albeit withholding some of them). The government does not execute an SCA warrant itself by conducting a search and seizing the emails directly in the same way the government might search a house and seize a personal computer, for example.

The Second Circuit disagreed, reasoning that the warrant required for a service provider to make a disclosure to the government under the SCA is, indeed, the same thing as is meant by the term

of art "warrant." As a result, the court concluded that no law developed in the subpoena context could apply to the SCA warrant, and the scope of the search would therefore be limited by the scope of the SCA's authority. Accordingly, the fact that Microsoft was physically located in the United States and subject to the jurisdiction of the SCA generally was not relevant. Instead, the operative issue is what conduct of Microsoft—i.e., which of Microsoft's services—is covered by the SCA and thus subject to a warrant issued under the SCA.

The court then addressed the SCA's scope. If the SCA does not reach outside of the United States, the court reasoned, the warrant could not reach outside of the United States either. The court concluded that the SCA does not "contemplate or permit extraterritorial application," reasoning that the "focus" of the SCA's warrant provisions is "protecting the privacy of the content of a user's stored electronic communications." In other words, the SCA is intended to protect the privacy of individuals in connection with the seizure of emails, and that privacy protection is intended to apply within the United States.

As a result, the activity permitted pursuant to any SCA warrant—e.g., a search of emails—also must apply only within the United States. Based on this analysis, the court had "little trouble" concluding that using the warrant to authorize the retrieval of emails stored abroad would constitute "an unlawful extraterritorial application" of the SCA.

Finally, the court confirmed that the activity at issue would, indeed, occur outside of the United States, reasoning in part that "the data is stored in Dublin, that Microsoft will necessarily interact with the Dublin datacenter in order to retrieve the information for the government's benefit, and that the data lies within the jurisdiction of a foreign sovereign [i.e., Ireland]." In other words, even if Microsoft accessed the emails from a U.S. workstation, the actual seizure of the emails would occur on a server in Dublin.

AFTERMATH AND IMPLICATIONS

Microsoft v. United States was closely watched because of privacy concerns raised by the governments of some countries in the European Union and by advocacy groups and others. A number of U.S.-based technology and media companies, as well as trade associations, advocacy groups and the government of Ireland itself, filed amicus briefs in favor of Microsoft's position in the case. The Irish government's brief, for example, argued "[f]oreign courts are obliged to respect Irish sovereignty" because Ireland cooperates with other states to fight crime and has enacted legislation giving effect to international treaties and instruments that provide for mutual legal assistance in criminal matters.

This ruling should be some comfort to U.S. companies that provide stored communications services, such as email, on a global basis. For now, at least, it appears U.S. law enforcement cannot directly access, via warrants issued under the SCA, information that: (1) belongs to people who are not in the United States; (2) is held by U.S.-based service providers; and (3) is stored on servers that are not within U.S. territory. The opinion does not, however, resolve all debates about cross-border data transfers and data access. In particular, the SCA is just one of many mechanisms by which the U.S. government can access information; there are other mechanisms that are, indeed, subpoena-based and thus not subject to the same strict territorial analysis.

Furthermore, the court did not resolve how the SCA warrant provisions would apply to data stored abroad but related to U.S. citizens or residents. While the U.S. legal regime has typically been territorially based, in the cloud-based digital age, a bright territorial line may not be viable. One possibility would be for the United States to adopt a regime that focuses not on the physical location of the data but on the physical location of the data subject (i.e., where the individual resides, as opposed to where the emails reside).

Otherwise, a singular focus on the location of the information itself might result in more governments implementing data localization requirements to ensure that they can access their residents' information. Because increased localization requirements can make it difficult to deliver cloud-based services, including email services, such requirements would ironically be just as detrimental to service providers as the prospect of a globalized SCA was prior to the Second Circuit's *Microsoft v. United States* decision.

In light of these considerations, it remains to be seen how the U.S. Justice Department, other governments and other industries will respond. In the near term, possibilities include a legislative fix or an appeal, which—in light of the current eight-member Supreme Court and the possibility of a 4-4 split decision that would leave the Second Circuit's ruling in place—would most likely be to the Second Circuit en banc.

One thing is clear: We have not seen the end of the debate over the reach of government authority in the digital age or over the concept of jurisdiction and territoriality when information can move across borders—and be moved across borders—in the blink of an eye.

EUROPEAN COMMISSION PUBLISHES DRAFT REGULATION PROHIBITING GEO-BLOCKING BY ONLINE TRADERS AND CONTENT PUBLISHERS

By Susan McLean and Holger Andreas Kastler

As part of the European Commission's Digital Single Market initiative, the European Commission has published

a draft Regulation aimed at preventing traders from discriminating against customers located in other EU Member States by denying those customers access to e-commerce sites, or by redirecting those customers to websites that offer inferior goods or sales conditions—a practice known as geo-blocking. The proposed new rules will benefit both consumers and businesses that purchase goods or services within the EU (excluding resellers).

The European Commission believes that geo-blocking and discriminatory practices undermine online shopping and cross-border sales within the EU.

The Regulation, which must still undergo review by the European Parliament and the Council of the EU, may change and is expected to be in force in 2017 (except the ban on discriminating against customers of electronically supplied services, which is expected to be effective beginning July 2018). When it is adopted, the Regulation will automatically take effect in all Member States without each Member State having to implement it into national law.

THE TRADERS TO WHOM THE REGULATION APPLIES

The Regulation will apply to all traders, (including small- and medium-sized enterprises and micro-enterprises) operating in the EU. Small businesses that fall under a national VAT threshold, however, will be exempt from certain provisions. The Regulation will also apply to traders established outside the EU to the extent that they sell or intend to sell goods or services to customers in the EU.

THE PROHIBITION AGAINST DISCRIMINATION

Traders must not discriminate against customers on the basis of their nationality, place of residence or place of establishment when selling (or seeking to sell) goods or services:

- in a Member State other than the Member State in which the customer resides or has its establishment;
- in the same Member State, but the customer is a national of another Member State; or
- in a Member State in which the customer is temporarily located without residing in that Member State or having a place of establishment there.

THE PROHIBITION AGAINST BLOCKING

A trader operating an online interface (such as a website or app) will not be permitted, through technology measures or otherwise, to block or limit customers' access for reasons related to the customer's nationality, place of residence or establishment. In addition, a trader will not be permitted to redirect a customer from one website to an alternative website without the customer's consent. And, if a customer consents to the redirection, the customer must still be able to access the original website.

THE PROHIBITION AGAINST DIFFERENT TERMS, GOODS OR SERVICES

A trader may not apply different terms and conditions to a customer based on that customer's nationality, residence or place of establishment. This ban applies to:

- sales of goods where the trader is based in a different Member State than the customer;
- all electronically supplied services (except services that involve providing access to copyright-protected content, as discussed below), e.g., cloud services and web hosting; and
- offline services provided at the trader's premises or in a location where the trader operates, where such site is in a different Member State than where the customer is a national, is resident or is established.

Note that the Regulation does not require traders to deliver goods cross-border, however. As long as it requires the same thing of all of its customers, a merchant may require a foreign customer to pick up goods in the Member State where the merchant is located, or in another Member State to which the merchant delivers.

THE PROHIBITION AGAINST DIFFERENT PAYMENT CONDITIONS

A trader may not apply different payment conditions to sales of goods or services within the EU, subject to certain criteria. However, a trader will still be free to decide which payment means it accepts from customers. And the Regulation does not address pricing, so traders will still be free to set prices in a non-discriminatory manner.

EXCEPTIONS

To the relief of content providers across the EU, the Regulation does not apply to copyrighted content. This is a departure from the Commission's original plans, and means that digital content providers (e.g., providers of audio-visual media, e-books, gaming apps and software) can continue to licence their content on a territorial basis (subject to portability obligations under the draft Regulation on cross-border portability and obligations under the proposed amendments to the Audiovisual Media Service Directive).

The Regulation also does not apply to financial services, transportation services, health care services or gambling.

There are also specific exceptions to the discrimination obligations, where required, to comply with applicable EU or Member State laws (e.g., applicable laws regarding the protection of children), but any such restrictions must be "precisely justified."

THE IMPACT OF BREXIT

The UK voted to leave the EU on June 23, 2016. However, until the UK government formally provides an Article 50 notice, the UK remains part of the EU and subject to EU law and regulation. Accordingly, if this Regulation comes into force in 2017, it will apply to the UK because it is

directly applicable in all EU Member States. Whether or not the law will continue to apply post-Brexit will depend on the Brexit model that the UK government adopts, which is not yet clear. It seems likely that this sort of law is one which the UK government would positively want to encourage—or at least the UK government would need to find some way to agree mutual recognition between the EU and the UK, because if the law doesn't apply to the UK, then it would mean that EU businesses could discriminate against UK customers.

WHAT TRADERS SHOULD DO NOW

Traders that will be affected by the proposed new law should start reviewing the technical features of their platforms, as well as their terms and conditions, including their payment terms, to identify whether they discriminate against customers based on their nationality, place of residence or place of establishment. Traders should also consider what changes their platforms and terms will have to undergo to ensure compliance with the new law so that, when the proposed law is adopted, they will have started to undertake the necessary preparations.

UK CONSUMER PROTECTION REGULATOR CRACKS DOWN ON UNDISCLOSED ENDORSEMENTS AND "CHERRY PICKING" REVIEWS ON SOCIAL MEDIA

By Susan McLean

Social media is reportedly rife with influencers promoting or reviewing products or services without disclosing compensation or other consideration that they've received for such endorsements. The Competition and Markets Authority (CMA), the UK's consumer protection regulator, is stepping up efforts to combat such undisclosed endorsements.

Following a ruling against an influencer marketing company, Social Chain Ltd, the CMA has warned 15 companies and 43 "social media personalities" who used Social Chain to publish content on social media that they could be in breach of UK consumer protection laws.

As we have discussed many times in Socially Aware, the advertising landscape has undergone a dramatic transformation over the past decade. The rise of social media and ever-increasing levels of Internet access across the world have made social media advertising a strong challenger to more traditional—and expensive—advertising methods, such as television advertising.

Of course, there is nothing novel in companies seeking to use celebrities to attract attention to and create excitement for their brand messages. But what has changed is the medium; when a consumer follows a celebrity on YouTube, Instagram, Facebook, Snapchat or Twitter (*especially* a social media personality who has become famous as a result of being on YouTube, Instagram, etc.), it's not always easy to distinguish between a genuine opinion and an advertisement.

According to the CMA, between March and July 2015, 19 marketing campaigns that Social Chain arranged involved undisclosed advertising. The regulator believed that various ads posted to Twitter, YouTube and Instagram may have been difficult for readers to "distinguish from other posts, conversations and jokes they appeared alongside."

Social Chain accepted the CMA's ruling and has agreed that all future campaigns will be clearly distinguishable from other social media content, in accordance with the UK's Consumer Protection from Unfair Trading Regulations 2008.

The rise of social media and ever-increasing levels of Internet access across the world have made social media advertising a strong challenger to more traditional—and expensive—advertising methods, such as television advertising.

WHAT CONSTITUTES ADVERTISING?

The CMA is concerned with "paid-for" advertising. The CMA interprets this term broadly; payment, for example, may include nonfinancial remuneration such as free samples, tickets or access to membership services.

A second key element is the degree of editorial control that the business supplying the product or service has over the content of the social media post or other endorsement. Behavior by a company that could indicate a sufficient degree of control includes supplying language that is to be partially or entirely reproduced verbatim by the social media influencer.

On the other hand, if a company provides a celebrity with a number of free samples of a product, and the celebrity subsequently posts an endorsement of such product on social media entirely on his or her own volition and using his or her own words, then that would not be considered by the CMA to be an act of "advertising" that product. (Of course, in other countries, it may be that a regulator would reach a different outcome in this scenario.)

How can advertisements be made distinguishable from other types of content?

The CMA has advised that an advertisement must be clearly identifiable to consumers. One method would be to make an explicit reference to the fact that the content is an advertisement. Simply writing "ad" or similar language in the description would suffice. Although such an explicit reference is not essential (e.g., it may be clear from the context that a post is an ad), adopting this method would certainly be the safest way to avoid attracting the CMA's attention.

ONLINE REVIEWS

The CMA also recently announced a ruling against clothing retailer WoolOvers for "cherry-picking" more favorable customer reviews for publication on its website. Over the period from December 2014 to November 2015, WoolOvers staff were instructed to approve only a selection of reviews, and none below 4 stars. This resulted in almost half of the reviews it received during the period going unpublished. In publicizing its ruling the CMA made clear that it's important that when consumers read reviews on a company's website they are given the complete picture. In particular, critical reviews must be published as well as those that praise the company's products and services.

Following these two rulings, the CMA has issued updated guidance on online reviews and an open letter to marketing agents and their clients about their obligations under consumer law concerning endorsements and reviews.

CONCLUSION

These CMA rulings, which reinforce previous guidance and enforcement actions from the UK's advertising regulator and recent guidance on endorsements and reviews from The International Consumer Protection and Enforcement Network (a network of consumer protection authorities from nearly 60 countries), should be a reminder to brands and marketers, once again, that, no matter how creative or cutting-edge their UK social media campaigns are, the campaigns remain subject to advertising standards.

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.