Volume 7, Issue 5, August 2016

SOCIALLY AWARE

BURTON AWARDS 2011 BEST LAW FIRM NEWSLETTER

THE SOCIAL MEDIA LAW UPDATE

IN THIS ISSUE

EDITORS

John F. Delaney
Aaron P. Rubin

CONTRIBUTORS

John F. Delaney
Aaron Rubin
Dina Roumiantseva
Jamie Levitt
Ken B. Nicholds
Anthony M. Ramirez
Mara Elyse Goodman
Andrew Serwin
Kai Bartolomeo
Claudia Maria Vetesi
Suhna Pierce
Adam Fleisher

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 discuss the impact online trolls are having on social media marketing; we revisit whether hashtags should be afforded trademark protection; we explain how an unusual New Jersey law is disrupting the ecommerce industry and creating traps for the unwary; we explore legal and business implications of the Pokémon Go craze; we examine a recent federal court decision likely to affect application of the Video Privacy Protection Act to mobile apps; we discuss a class action suit against an app developer that highlights the legal risks of transitioning app customers from one business model to another; and we describe how Europe's Right to Be Forgotten has spread to Asia.

All this—plus infographics illustrating the enormous popularity of Pokémon Go and the unfortunate prevalence of online trolling.

Trolling Statistics

28% of Americans admit to online trolling.[1]

65% of 18-to-29-year-olds have experienced online harassment.[2]

18-29 yrs

77% of Americans believe that anonymity fuels online trolling.[3]

27% of Internet users have been insulted online.[2]

Once a week

Americans are most likely to encounter trolls at least once a week on chat boards (45%), social media (39%) and blogs (39%).[3]

SOURCES

1. http://www.huffingtonpost.com/2014/10/20/internet-trolls-survey_n_6014826.html?utm_hp_ref=mostpopular
2. https://www.entrepreneur.com/article/242924
3. https://today.yougov.com/news/2014/10/20/over-quarter-americans-admit-malicious-online-comm/

ARE ONLINE TROLLS RUINING SOCIAL MEDIA MARKETING?

By John Delaney

Earlier this year, I helped moderate a lively panel discussion on social media business and legal trends. The panelists, who represented well-known brands, didn't agree on anything. One panelist would make an observation, only to be immediately challenged by another panelist. Hoping to generate even more sparks, I asked each panelist to identify the issue that most frustrated him or her about social media marketing. To my surprise, the panelists all agreed that online trolls were among the biggest source of headaches.

This contentious group proceeded to unanimously bemoan the fact that the comments sections on their companies' social media pages often devolve into depressing cesspools of invective and hate speech, scaring off customers who otherwise would be interested in engaging with brands online.

And it isn't just our panelists who feel this way. Many online publishers have eliminated the comments sections on their websites as, over time, those sections became rife with off-topic, inflammatory and even downright scary messages.

For example, *Above the Law*, perhaps the most widely read website within the legal profession, recently canned its comments section, citing a change in the comments' "number and quality."

The technology news website *Wired* even put together a timeline chronicling other media companies' moves to make the same decision, saying the change was possibly a result of the fact that, "as online audiences have grown, the pain of moderating conversations on the web has grown, too."

Both brands and publishers are right to be concerned. Unlike consumers who visit an online branded community to voice a legitimate concern or share an invaluable insight, trolls "aren't interested in a productive outcome." Their main goal is harassment, and, as a columnist at *The Daily Dot* has observed, "People are generally less likely to use a service if harassment is part of the experience." That's especially true of online branded customer communities, which consumers mainly visit to get information about a brand (50%) and to engage with consumers like themselves (21%).

Of course, it's easy for a brand to eliminate the comments section on its own website or blog. But, increasingly, brands are not engaging with consumers on their own online properties; they're doing it on Facebook, Instagram, Twitter and other third-party social media platforms, where they typically do not have an ability to shut down user comments. Some of these platforms, however, are taking steps to rein in trolls or eliminate their opportunities to post disruptive comments altogether.

The blog comment–hosting service Disqus, for example, recently unveiled a new platform feature that will allow users to "block profiles of commenters that are distracting from their online discussion experience." The live video-streaming app Periscope also recently took measures to rein in trolls, enabling users to flag what they consider to be inappropriate comments during a broadcast. If a majority of randomly selected viewers vote that the flagged comment is spam or abusive, the commenter's ability to post is temporarily disabled. And even Facebook, Instagram and Twitter have stepped up their efforts to help users deal with harassment and unwanted messages.

The comments sections on companies' social media pages too often devolve into depressing cesspools of invective and hate speech, scaring off customers who otherwise would be interested in engaging with brands online.

Brands, however, are seeking a greater degree of control over user comments than what is being offered even by Disqus and Periscope. Given that branded content and advertising are crucial components of many social media platforms' business models, we can expect to see platforms becoming more willing to provide brands with tools to address their troll concerns.

In fact, the user-generated content site Reddit has already taken steps in this direction. Because of its notorious trolling problem, Reddit has had trouble leveraging its large and passionate user base. Last year, in an effort to capitalize on the platform's ability to identify trending content and create a space where brands wouldn't be afraid to advertise, Reddit launched Upvote, a site that culls news stories from Reddit's popular subgroups and doesn't allow comments.

Other platforms will presumably follow Reddit's lead in creating comment-free spaces for brands. Although this may prove to be good news for many brands, one can't help but feel that this inevitable development undermines—just as trolls have undermined—the single most exciting and revolutionary aspect of social media for companies: the ability to truly engage one-on-one with customers across the entire customer base.

(**Note**: This article originally appeared in *MarketWatch*.)

#TRADEMARKS?: HASHTAGS AS TRADEMARKS REVISITED

By Aaron Rubin and Dina Roumiantseva

Since our previous article on the emerging issue of trademark rights in hashtags, the use of hashtags in social media marketing has continued to grow. Described as the "ignition keys to a social media keyword search," hashtags can be powerful tools for creating communities around a brand. Indeed, recent scholarship suggests that modern brand narratives are written in collaboration with consumer communities rather than by brand owners acting alone.

A catchy hashtag creates its own social media channel, and brand owners naturally want to prevent competitors from hijacking the content stream tied to their cleverly crafted messages. To safeguard the investment in this narrative, companies are increasingly seeking trademark protection for their hashtags. Applications for hashtag trademarks continue to soar, with over 1,042 hashtag trademark applications in 2015 in the United States alone. However, despite the United States Patent and Trademark Office's (USPTO) guidance regarding hashtag trademarks in its Trademark Manual of Examining Procedure (TMEP), hashtags continue to pose challenges for both USPTO examiners and the courts.

At the USPTO, examination and registration of hashtag marks remain somewhat inconsistent. As we noted in our previous article, the USPTO has addressed the issue of hashtags' ability to function as trademarks in the "Hashtag Marks" section of the TMEP. In essence, the TMEP states that the hashtag symbol should be ignored by the examiner and the hashtag mark should be examined in the same manner in which any other tag line or phrase would be. In other words, according to the USPTO, a hashtag is no more—but also no less—capable of functioning as a trademark than the non-hashtag form of the relevant tag line or phrase would be. But does this approach ignore some unique features of hashtag marks?

First, while descriptiveness is an issue for both hashtag and non-hashtag marks, the fact that hashtag marks also function as online search terms would seem to increase the need for a hashtag to have a close and obvious connection to a particular brand if it is to be recognized as a trademark—i.e., an identifier of the source of goods and services—and not merely a search term. For example, the word "Tasty" may be merely descriptive when used on a package of bread, but #Tasty is arguably even less distinctive when used only in a social media campaign, considering that the hashtag does not actually appear on the product and, considered as a search term, could be relevant to any number of topics.

The TMEP notes this problem and instructs that #Skater for skateboarding equipment would not be registrable as merely descriptive. However, in practice, the USPTO has not always been entirely consistent in assessing the descriptiveness of hashtag trademarks. For example, the USPTO has allowed #LetsBowl for bowling balls and #Smart for clothing without raising a descriptiveness objection. The USPTO also allowed Abercrombie & Fitch to register #SoCalStylist for retail store services featuring clothing and accessories, and a non-profit to register #KickHunger for promoting public awareness of hunger and hunger relief. But the USPTO found #WeatherWednesday for an online newsletter about the weather and #MusicVideoMonday for advertising services and mobile marketing to be merely descriptive, allowing only registration on the supplemental register.

Second, the fact that a hashtag often appears only on social media rather than on the goods themselves or in advertising raises questions regarding what constitutes an acceptable specimen for a hashtag mark. The USPTO has not formulated a clear policy on this issue. The TMEP notes that if #SewFun was the subject of a trademark application for "instruction in the field of sewing" with a specimen consisting of a screenshot of a social networking site used to organize user comments about sewing classes that the applicant offers, the mark would be *refused* registration for failure to function as a service mark. Accordingly, the USPTO rejected the initial specimen for #LeadershipFlow in connection with business education services that consisted of the applicant's website with posts about business topics. However, the USPTO allowed Procter & Gamble to register #LikeAGirl for "providing information in the field of female empowerment, anti-gender discrimination via social media" with a screenshot of its Twitter page as a specimen.

Only a handful of court decisions have dealt with the subject of trademark rights in hashtags to date, with similarly inconsistent outcomes. As we previously wrote, a district court in Mississippi held that use of the tags #FratCollection and #FraternityCollection by a competitor of the clothing maker Fraternity Collection was sufficient to state a claim for false advertising under the Lanham Act and for trademark infringement under state law. However, in a recent California case, *Eksouzian v. Albanese*, the court concluded that a competitor's use of a hashtag did not violate a settlement agreement on trademark usage between the parties because the hashtag was "merely a functional tool."

The application of trademark law to hashtags and the rapidly evolving social media landscape are still in their very early stages.

The parties in *Eksouzian* had jointly developed a compact vaporizer pen, but later separated and entered into a settlement agreement pursuant to which the plaintiffs were permitted to use the terms "Cloud" or "Cloud Vapes" as trademarks, but not in such close association with the words "pen" or "penz"—common descriptors for compact vaporizers—as to form a unitary trademark. Plaintiffs then used the hashtags #cloudpen and #cloudpenz in connection with promotional contests on social media. The court found that plaintiffs did not breach the settlement agreement because "hashtags are merely descriptive devices, not trademarks, unitary or otherwise, in and of themselves" and use of the hashtag "is merely a functional tool to direct the location of Plaintiffs' promotion so that it is viewed by a group of consumers, not an actual trademark." This conclusion seems to be at odds with the USPTO's willingness to register hashtags as trademarks.

In another recent case, *Public Impact, LLC v. Boston Consulting Group, Inc.*, a Massachusetts court came to the opposite conclusion. In that case, Public Impact, LLC, an education policy and management consulting firm that owns a federal registration for the mark PUBLIC IMPACT, sought a preliminary injunction to prevent the defendant, Boston Consulting Group (BCG), from using the hashtag #PublicImpact and the username @4PublicImpact on social media. After determining that BCG had not submitted sufficient evidence to show that "public impact" is generic for consulting services in light of the fact that Public Impact's federal registration had attained incontestable status, the court concluded that BCG's use of the username and hashtag was likely to constitute trademark infringement, particularly given the similarity of the services provided by the two organizations. Accordingly, the court enjoined BCG from using the phrase "public impact" with two or fewer letters, numbers or characters appended in any form on social media or in other commercial activities.

In sum, the application of trademark law to hashtags and the rapidly evolving social media landscape are still in their very early stages. With regard to federal registration, one scholar has argued that the USPTO should treat hashtag marks as "primarily merely a hashtag" until the applicant can establish that the mark actually functions as a source indicator, an approach that could avoid some of the inconsistencies seen in the registration process today. The bigger questions regarding the scope of protection afforded to hashtag marks and the analysis of trademark infringement involving use of hashtags marks on social media, however, have yet to be resolved.

CONTROVERSIAL NEW JERSEY CONSUMER PROTECTION LAW CREATES A POTENTIAL "GOTCHA" FOR ECOMMERCE COMPANIES

By John Delaney, Jamie Levitt, Ken B. Nicholds, Anthony M. Ramirez and Mara Elyse Goodman

If your company is involved in selling products or services to consumers in New Jersey over the web or through mobile apps, you'll want to read this article.

In what amounts to a feeding frenzy, plaintiffs' lawyers are working overtime bringing class action suits against ecommerce companies, alleging that their online terms and conditions violate New Jersey's unusual Truth-in-Consumer Contract, Warranty and Notice Act (TCCWNA). Some of the online retailers to have been sued include Victoria's Secret, Bed Bath & Beyond and TOYS "R" US, with more suits being filed every day.

Unlike most consumer protection laws, the TCCWNA focuses specifically on the contractual terms governing certain transactions with consumers, imposing limitations on such terms—*even if such contractual terms are governed by the law of a state other than New Jersey*—creating a potential gotcha for etailers who are based outside of New Jersey and who traditionally have their online terms and conditions reviewed only by lawyers admitted to practice in the state whose laws govern such terms and conditions.

Although the TCCWNA was enacted in 1981, it has only recently achieved notoriety, as more and more plaintiffs' lawyers have embraced the statute due to its broad scope and its statutory penalty of not less than $100 per violation without the need to prove actual harm.

New Jersey's TCCWNA is creating a feeding frenzy among plaintiffs' lawyers.

OVERVIEW OF THE TCCWNA

New Jersey adopted the TCCWNA over 30 years ago not to create new rights for consumers, but rather to "bolster[] rights and responsibilities established by other laws," particularly those established by New Jersey's Consumer Fraud Act (CFA). Observers have noted that the number of TCCWNA cases has been increasing in the last few years, particularly since 2013 when the Supreme Court of New Jersey in *Shelton v. Restaurant.com, Inc.* found that online certificates or coupons were subject to TCCWNA rules and opened the door to TCCWNA class actions stemming from ecommerce.

The TCCWNA applies where a company is a "seller, lessor, creditor, lender or bailee," offering its services to a "consumer" or "prospective consumer" in New Jersey. A "consumer," under the TCCWNA, is defined as "any individual who buys, leases, borrows, or bails any money, property or service which is primarily for personal, family or household purposes." Indeed, courts have emphasized that the TCCWNA is inapplicable unless the plaintiffs are consumers.

The text of the TCCWNA prohibits three types of provisions in consumer contracts, warranties, notices and signs.

First, it prohibits provisions violating "clearly established" legal rights of a consumer or responsibilities of a seller, lessor, creditor, lender or bailee. These rights and responsibilities may arise from federal or state law. For example, one court found that provisions restricting limitations periods for initiating lawsuits, asserting counterclaims or raising affirmative defenses violate consumers' rights under federal and New Jersey procedural rules.

Second, the TCCWNA prohibits provisions waiving a consumer's rights under the TCCWNA. In *Johnson v. Wynn's Extended Care, Inc.*, for example, the U.S. Court of Appeals for the Third Circuit held that a provision in a service contract that prevented the recovery of attorneys' fees and costs constituted a waiver of a consumer's rights under the TCCWNA and was therefore prohibited.

Note, however, that at least two cases have found that a claim under the TCCWNA cannot be based merely upon an omission. As one court noted, the statute's use of the term "includes" suggests that only a statement affirmatively "included" in the consumer contract, warranty, notice or sign should give rise to liability; in addition, the legislative history does not include any examples of an omission triggering liability.

Third, the TCCWNA prohibits blanket "inapplicable in some jurisdictions" savings clauses (e.g., phrased "void where prohibited")—though, notably, it does not prohibit such savings clauses in any warranty. In order for a savings clause to be acceptable under the TCCWNA, the statute requires the clause to specify which provisions, if any, are unenforceable in New Jersey.

In one recent case, *Martinez-Santiago v. Public Storage*, the following language was found to be in violation of the TCCWNA's prohibition against overly broad savings clauses: "If any provision of this [agreement] shall be invalid or prohibited under [the law of the state where the applicable premises are located], such provision shall be ineffective only to the extent of such prohibition or invalidity, without invalidating the remainder of such provision or the remaining provisions."

Certain courts, however, have refused to find such a violation of the TCCWNA when the consumer contract, notice or sign is only available within New Jersey, or when the clause uses the alternative "to the extent permitted by law" phrasing, as discussed below.

TCCWNA'S POTENTIAL DANGER TO ONLINE COMPANIES

The TCCWNA is potentially dangerous for companies operating online for at least three reasons.

First, plaintiffs' lawyers are pushing for an extremely broad application of the statute. They argue that the TCCWNA applies to almost every company providing consumer products online that are available to New Jersey residents, and to any "written consumer contract" and "written consumer warranty, notice or sign" made available to these residents—presumably encompassing nearly all material displayed or offered by a company online.

Second, as noted above, the TCCWNA may expose companies located outside of New Jersey (but whose online websites can be accessed within the state) to claims stemming from any applicable "clearly established" federal or New Jersey state right or responsibility, effectively requiring companies based outside of New Jersey to develop expertise on all potentially applicable New Jersey laws (even if their website terms of use purport to be governed by another state's laws and have been carefully drafted and reviewed by lawyers admitted to practice in such state).

Think about it: If every state had a law similar to the TCCWNA, every etailer would need to have its online Terms of Use reviewed by as many as *50 different lawyers*. The result would essentially be a full employment act for attorneys across the country.

Third, the TCCWNA is potentially dangerous for companies because it provides an "aggrieved consumer" with the option to seek recovery of a civil penalty of not less than $100. This means the penalties in class actions—especially the penalties in class actions over online terms and conditions—could add up quickly. The text of the statute also allows for actual damages, reasonable attorneys' fees and court costs *in addition* to the civil penalty, and further states that such remedies are cumulative and do not preclude recovery available under other laws.

SOME GUIDANCE FOR ONLINE COMPANIES FROM EMERGING TCCWNA CASE LAW

Because claims arguing that online terms and conditions violate the TCCWNA have been filed only recently, there is only sparse guidance from the courts on how online companies selling into New Jersey can protect against these lawsuits.

Moreover, any such company, if it has not already done so, *should promptly contact New Jersey counsel for advice on how to ensure its online terms and conditions are compliant with the TCCWNA*.

With those important caveats in mind, recent court decisions applying the TCCWNA do highlight some potential precautionary measures for website operators.

For example, *as a first line of defense*, it may be prudent for companies to include, and seek to bolster the enforceability of, an arbitration provision and a related class action waiver clause in their online terms and conditions. As an example, in one TCCWNA case, the Supreme Court of New Jersey indicated that an arbitration provision would have been enforceable if it had clearly and unambiguously notified the consumer that she was waiving her statutory right to seek relief in a court of law. While there is no prescribed wording for a valid arbitration provision, one New Jersey court found the following arbitration notice to be acceptable:

> The parties to this agreement agree to arbitrate any claim, dispute, or controversy, including all statutory claims and any state or federal claims, that may arise out of or relating to the [subject matter of the agreement]. By agreeing to arbitration, the parties understand and agree that they are waiving their rights to maintain other available resolution processes, such as a court action or administrative proceeding, to settle their disputes.

As a second line of defense, it may be prudent for companies, working with New Jersey counsel, to review and potentially revise their online contracts, warranties and notices in light of TCCWNA cases to date. One approach suggested by existing TCCWNA case law is that businesses can avoid violating the TCCWNA's prohibition on blanket "inapplicable in some jurisdictions" savings clauses by using different language in their savings clauses to achieve the same result. As noted above, the text of the TCCWNA prohibits savings clauses that state that certain terms "may be void, unenforceable or inapplicable in some jurisdictions" if such clauses do not identify which terms are or are not void, unenforceable or inapplicable in New Jersey. In *Kendall v. CubeSmart L.P.*, however, the United States District Court for the District of New Jersey found that companies could use savings clauses that "attempt . . . to conform to New Jersey law." Citing several cases, it held that the phrases "to the extent permitted by law," "in the manner permitted by applicable law," "allowed by applicable law" and "or as otherwise permitted by applicable law" were acceptable in savings clauses under the TCCWNA.

Even if companies adjust their savings clauses as suggested by TCCWNA case law, it may still be prudent to pay particular attention to any language in their online contracts, warranties and notices that may violate "clearly established" legal rights, with particular attention to language that:

- *Waives a consumer's right to recover attorneys' fees or requires litigation costs to be split. Current TCCWNA case law indicates that companies should be careful of clauses that explicitly waive a consumer's right to recover his or her attorneys' fees or state that "[e]ach party shall pay the fees of its own attorneys."*

- *Limits liability of the company for personal injuries or property damage. The enforceability of such limitations will vary based on the situation, including variance from industry to industry. For example, on the one hand, a limitation of liability in a rental agreement for storage space, which released the storage company from liability "for any personal injuries or property damage sustained by Customer and/or Customer's guests while on" the company's property, was found by a court to violate the TCCWNA because, under applicable New Jersey law, storage companies are under a duty to maintain their premises for consumers. On the other hand, a similar limitation of liability in a gym membership agreement was found by a court not to violate the TCCWNA because, the court reasoned, consumers are deemed to have assumed certain risks for personal injury on gym premises under New Jersey law.*

- *Indemnifies the company against losses resulting from the company's own negligence. For example, a rental agreement offered by a storage company that included consumer indemnification of the company for "any and all manner of claims for damages or lost property or personal injury" was found by a court to violate the TCCWNA.*

- *Restricts claim limitation periods. At least one court has reasoned that the Federal Rules of Civil Procedure and New Jersey Court Rules dictate statutes of limitation on claims, from which companies cannot derogate, and therefore any attempt to shorten a consumer's claim limitation period would violate the TCCWNA.*

- *In addition to the above, current TCCWNA case law suggests that companies should present disclaimers and limitations of liability, in particular, conspicuously to consumers (e.g., use capital letters).*

THE *SPOKEO, INC. V. ROBINS* DECISION AND ITS POTENTIAL IMPACT ON TCCWNA LITIGATION

Although, as noted, the TCCWNA allows aggrieved consumers to elect a $100 civil remedy instead of their actual damages, the recent U.S. Supreme Court decision in *Spokeo, Inc. v. Robins* may make it more difficult for plaintiffs to maintain TCCWNA class actions *in federal court* where concrete and particularized harm has not been established.

The *Spokeo* case arose out of a claim by Robins that Spokeo, an operator of a "people search engine" that gathers and provides personal information about individuals to users, sold inaccurate information in violation of the Fair Credit Reporting Act. The U.S. Supreme Court held that standing to sue in federal court, even in the context of a statutory violation, requires proof of "concrete and particularized" harm inflicted on each individual plaintiff. It also held that "particularized" harm means "personal and individualized"—a relatively high threshold for class action plaintiffs claiming statutory violations. In fact, the First Circuit recently held in *Hochendoner v. Genzyme Corp.* that plaintiffs did not satisfy the "particularized harm" requirement because the plaintiffs' alleged injuries due to the shortage of a drug could not be linked to any specific plaintiff, and therefore the class actions were dismissed. At least one company has even submitted the *Spokeo* decision in support of its motion to dismiss in a case filed by a New Jersey consumer in federal court alleging that the company's online terms and conditions were in violation of the TCCWNA.

As it is too soon to definitively conclude how *Spokeo* will affect TCCWNA class actions, ecommerce companies will want to closely monitor TCCWNA developments, including any legislative initiatives that may result from recent lobbying efforts. In the meantime, companies would be well advised to review their online terms and conditions carefully with qualified counsel—indeed, the sharp increase in TCCWNA cases presents an opportunity for all website operators and mobile app developers to take a look at their terms and conditions and make sure that they are up to date.

AUGMENTING REALITY: A POKÉMON GO BUSINESS AND LEGAL PRIMER

By John Delaney and Aaron Rubin

We have become inured to the sight of people staring at their phones rather than engaging with one another or enjoying their real-life surroundings. But, over the past two weeks, enslavement to mobile devices rose to new levels, with smartphones and tablets actually propelling users' movements in the real world as opposed to merely distracting them from it.

Unless you've been off the grid this month, you know that the force mobilizing these seemingly possessed pedestrians (and drivers!) has been

Gotta Catch'Em All

Pokémon Go generated **$200 million** in revenue within one month of its release, breaking the record formerly held by Clash Royale (**$125 million**) and, before that, Candy Crush Soda Saga (**$25 million**).[1]

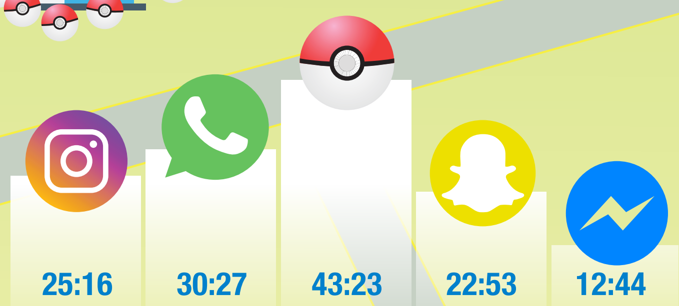
Men from 21 to 27 years old are the game's biggest users.[2]

At one point **25 million** people were actively using Pokémon Go.[3]

The game has been downloaded **100 million times**.[4]

The first person to catch every single Pokémon currently available in the U.S. walked **129 miles** to achieve that goal.[5]

The manager of one restaurant located near Pokémon Go players' activity reported a **75% increase in sales**.[6]



Two days after the game's release, users were spending an average of **43 minutes**, **23 seconds a day** playing the game. That's more time than they were spending on than WhatsApp (30:27), Instagram (25:16), Snapchat (22:53) and Messenger (12:44).[6]

SOURCES

1. http://www.techtimes.com/articles/172909/20160808/pok%C3%A9mon-go-beats-candy-crush-ends-historic-month-with-record-200-million-in-revenue.htm
2. http://www.adweek.com/news/advertising-branding/infographic-pokemon-go-could-be-what-farmville-never-was-successful-172626
3. http://www.nme.com/filmandtv/news/has-pok-mon-go-peaked-already-daily-active-users-/413271
4. https://techcrunch.com/2016/08/01/pokemon-go-passed-100-million-installs-over-the-weekend/?ncid=rss
5. http://www.rollingstone.com/culture/news/meet-brooklyn-guy-who-beat-pokemon-go-w431051
6. http://www.businessinsider.com/pokmon-gobigger-than-tinder-overtake-twitter-similarweb-data-stock-price-nintendo-niantic-2016-7?utm_source=feedly&utm_medium=webfeeds

Pokémon Go, an app that has been downloaded more than 15 million times. Pokémon Go is currently boasting more daily users than Twitter, despite having been launched on July 6, 2016, making it *the most popular mobile game of all time*.

Despite all this, if you happen to be, umm, *over a certain age* (i.e., you're not a Millennial or younger), you may be a bit mystified as to what this Pokémon Go thing is all about. Accordingly, we put together this primer on Pokémon Go, including some observations regarding potential legal issues raised by the app.

How the Game Works

Pokémon Go is an augmented reality game that uses the device's ability to track time and location and shows the user a map of his or her real-life surroundings. As the player moves around, the game superimposes animated Pokémon characters onto the screen over a view of the player's real-life surroundings as seen through his or her mobile device's camera. The more characters the player catches, the higher his or her ranking rises.

The game is free to download from online app stores but, as players progress, they need Pokémon coins to enable certain functions. While the game allows players to earn coins over time, the fastest way to acquire them is by purchasing them. Such in-app purchases are real money makers, expected to account for more than $50 billion in industry-wide revenue this year.

WHO'S BEHIND IT

The funds that players are plunking into Pokémon Go are likely to add up to real money for the companies behind the app, a joint project of The Pokémon Company, which is 32% owned by Nintendo, and Niantic Inc., a spinout from Alphabet Inc.

Since the app's recent release, shares in Nintendo—a company that has struggled in recent years as a result of its reluctance to embrace mobile games—have risen 56%. The game has also significantly strengthened the financial position of Unity Technologies, the company that owns the game engine software that provides basic functionality for Pokémon Go (and for approximately 31% of the 1,000 top-grossing mobile games).

PERKS AND PITFALLS (SOME, UNFORTUNATELY, LITERAL)

Pokémon Go is being hailed as boon for small businesses; to drive foot traffic, merchants are paying the app a $10 daily fee for items called lures, which attract users. It's also being lauded for incentivizing some players to exercise and for relieving users' depression and social anxiety. Of course, the app is also creating problems and drawing its share of controversy.

Safety concerns have arisen as players who won't look away from their mobile devices have run-ins with their real-life physical surroundings, cutting and bruising themselves, getting into driving accidents and even falling off cliffs. These incidents have prompted a police department in Texas to post to social media a list of safety reminders for Pokémon Go users.

The list advises players to "tell people where you're going if it is somewhere you've never been"—wise advice in light of police reports describing Missouri armed robbers' use of the game's geolocation feature "to anticipate the location and level of seclusion of unwitting victims."

And, while some columnists have deemed the game educational because many of its so-called PokéStops (places where players can get free in-game items) are famous landmarks and historical markers that allow "players to learn about their community and its history," some of those PokéStops, such as the Holocaust Museum, have objected, maintaining that playing the game on their property is inappropriate. They are frustrated by the fact that they have no control over their PokéStop designation.

LEGAL ISSUES

Despite the app being so new, it is already raising legal concerns. Some of the key concerns include the following:

Privacy

The Pokémon Go app has been dogged by privacy concerns. When it was first launched, the Pokémon Go app requested permission to access all of the data associated with the player's Google accounts (including emails, calendar entries, photos and stored documents). The app's first update, available since at least July 12, 2016, remedied that problem and now asks people downloading it for permission to access only their Google IDs and email addresses.

The more limited-information-access permission terms—which downloaders of the original version of Pokémon Go can only adopt by downloading the update, signing out and signing back in—haven't stopped U.S. Senator Al Franken from penning a letter to Niantic's CEO John Hanke requesting Niantic to answer a series of questions to "ensure that Americans'—especially children's—very sensitive information is protected."

> **Any innovative technology that becomes a worldwide phenomenon overnight is bound to raise legal concerns.**

Product Liability

And what about the aforementioned injuries that people have sustained while playing Pokémon Go? Can Pokémon Go's developers be held liable for such injuries? At least one car accident victim is suing another popular social media app, Snapchat, for the traumatic brain injuries he suffered when he was struck by a car driven by a Georgia woman allegedly trying to use the Snapchat speed filter—a feature that tracks how fast the app's user is moving and rewards points to users who submit photos of their speed.

Trespass

There's also the question of property rights. In some cases, owners of the physical real estate sites that have been designated as PokéStops have complained about the traffic and other nuisances caused by the players. As a result, Niantic is accepting requests for removal of PokéStops from property owners, but removal isn't guaranteed.

Of course, app users who enter upon another's land without permission may be subject to trespassing claims. But could the companies behind the game also be liable for trespass? As *The Guardian* points out, "A Pokéstop cannot be 'on private property.' A PokéStop does not exist: it is a latitude and longitude stored on Niantic's servers, interpreted by the Pokémon Go client which then represents it as a circle hovering over a stylized Google Map of the area surrounding the player."

It *is* possible to recover in trespass for an intangible invasion of property, but whether a real estate owner's exclusive rights to his or her property extends to cyberspace remains to be seen.

STEPS TAKEN TO MITIGATE LEGAL RISKS

Pokémon Go's owners have taken steps to limit their potential legal liability. For example, a warning screen on the app advises users to pay attention to their real-world surroundings. And Pokémon Go's detailed, robust Terms of service attempt to limit the potential liability of the companies behind the app. In addition to a $1,000 liability cap and a mandatory arbitration provision, the terms of service contain an entire "Safe Play" section, which states in part that, as a player, you "agree that your use of the App and play of the game is at your own risk, and it is your responsibility to maintain such health, liability, hazard, personal injury, medical, life, and other insurance policies as you deem reasonably necessary for any injuries that you may incur while using the Services. You also agree not to use the App to violate any applicable law, rule, or regulation (including but not limited to the laws of trespass)."

Pokémon Go's Terms of Service, however, don't do anything to limit the liability of the game's *players*. As noted above, users could be liable for trespass and for any harm that others suffer as a result of players' use of the app (especially careless use, such as playing while behind the wheel of a car).

THE UPSHOT

Any innovative technology that becomes a worldwide phenomenon overnight is bound to raise legal concerns. But, as we've noted here at *Socially Aware*, such concerns often turn out to be overblown. The real significance of Pokémon Go is ultimately a business, rather than a legal, story: thanks to the app, millions of consumers around the world have now embraced augmented reality technology. Lawsuits will inevitably follow in the wake of Pokémon Go's success but, more importantly, so will millions of dollars of investment in new augmented reality applications. As a result, in what could be a very short amount of time, the integration of augmented reality into nearly every facet of our everyday life will become, well, a reality.

[Authors' Note: We would like to thank Luke D. (age 13), Ben R. (age 12), Alfredo M. (age 10) and Dylan J. (age 9) for the invaluable research that they contributed to this blog post.]

FIRST CIRCUIT ISSUES POTENTIALLY SIGNIFICANT RULING ON FEDERAL VIDEO PRIVACY STATUTE'S APPLICATION TO MOBILE APPS

By Andrew Serwin and Kai Bartolomeo

The First Circuit Court of Appeals' recent decision in *Yershov v. Gannett Satellite Information Network, Inc.* may carry important implications for mobile app providers seeking to navigate federal privacy laws—in particular, the Video Privacy Protection Act of 1988 (VPPA).

Although *Yershov* is not the first case to consider how the VPPA applies to mobile apps, the opinion contains two key holdings regarding (1) the scope of protectable personally identifiable information and (2) the treatment of free app downloaders under the statute.

> In the end, the panel concluded that qualifying as a "subscriber" requires some kind of relationship between the individual and the video provider that gives the individual some form of special access to the video content.

THE VPPA

The VPPA was passed in 1988, after the video rental history of then–Supreme Court nominee Judge Robert Bork was disclosed in a newspaper article during debate over his nomination. Quoting the VPPA, the *Yershov* opinion explains that the statute is intended to preserve personal privacy in connection with the rental, purchase or delivery of video and audio materials and creates a "civil remedy against a 'videotape service provider' for 'knowingly disclos[ing], to any person, [personally identifiable information] concerning any consumer of such provider.'" Of relevance in *Yershov*, the statute defines "consumer" as "any renter, purchaser, or subscriber of goods or services from a videotape service provider." The VPPA defines personally identifiable information to "include[] information which identifies a person as having requested or obtained specific video materials or services from a videotape service provider."

CASE BACKGROUND

According to the allegations in Yershov's operative complaint, which were taken as true for purposes of the First Circuit's opinion, Yershov downloaded the free *USA Today* mobile app ("the app") on his Android mobile device in late 2013. The app is offered by Gannett via the Google Play Store and allows the user to access various *USA Today* media and content, including videos, on the user's mobile device.

Yershov claims that he watched numerous video clips on the app. Each time, Yershov's operative complaint states, Gannett and its third-party marketing and analytics vendor collected three pieces of data: (1) the title of the video Yershov viewed; (2) the GPS coordinates of the device Yershov used; and (3) Yershov's unique Android ID. According to Yershov, the vendor used this information to create "digital dossiers" for Yershov and similarly situated users, which Gannett in turn used to provide targeted advertising. Yershov says he never consented to the collection of this data. He filed a putative class action lawsuit as a result, claiming that Gannett's actions violated the VPPA.

Gannett successfully moved to dismiss Yershov's VPPA claim. The district court held that the information Gannett collected and disclosed to its vendor constituted personally identifiable information but nevertheless concluded that Yershov was not a "consumer" with a right of action under the VPPA because he failed to allege that he was a renter, purchaser or subscriber of Gannett's video content. Yershov appealed.

FIRST CIRCUIT REVIVES YERSHOV'S CLAIM

The First Circuit reversed the district court's dismissal order and remanded for further proceedings.

First, the panel agreed with the district court that the information conveyed to the vendor by Gannett constituted personally identifiable information under the VPPA. According to the panel, the VPPA's "abstract formulation" of personally identifiable information does not require the information at issue to "explicitly name[] a person" to come within the ambit of the statute. Rather, it is sufficient if the information "effectively reveal[s] the name" or identity "of the video viewer" without too much uncertainty or "yet-to-be-done, or unforeseeable detective work."

Because Yershov alleged that Gannett's vendor could connect the GPS coordinates and Android ID with a given person's "name, address, phone number, and more," the panel concluded that he sufficiently alleged a "firm and readily foreseeable" link between the data collected and the user's identity.

Second, the panel addressed the "closer question" of whether Yershov is a "subscriber" and, therefore, a consumer under the VPPA. Lacking a clear statutory definition, the panel evaluated various dictionary definitions of "subscribe," which "include as an element a payment of some type and/or presume more than a one-shot transaction."

The panel expressly rejected the notion that the term "subscriber" incorporated a monetary payment requirement. Requiring monetary payment as an element, the panel reasoned, would render "subscriber" superfluous since the statute also lists "purchaser" and "renter" under its definition of "consumer," and those terms necessarily imply the payment of some monetary amount. According to the panel, "Congress would have had no need to include a third category of persons [i.e., subscribers] protected under the Act if it had intended that only persons who pay money for videos be protected."

The panel also found it significant that, in 2012, Congress considered the impact of the VPPA on video content in the age of the Internet and left the definition of "consumer" untouched—an indication, according to the panel, that "Congress understood its originally-provided definition to provide at least as much protection in the digital age as it provided in 1988."

In the end, the panel concluded that qualifying as a "subscriber" requires some kind of relationship between the individual and the video provider that gives the individual some form of special access to the video content. As the panel stated:

> [B]y installing the App on his phone, thereby establishing seamless access to an electronic version of *USA Today*, Yershov established a relationship with Gannett that is materially different from what would have been the case had *USA Today* simply remained one of millions of sites on the web that Yershov might have accessed through a web browser.

LOOKING AHEAD

The *Yershov* decision is not without its critics. Its holdings conflict with the opinions of other courts that have considered similar issues.

For example, federal district courts, including the Northern District of California and the District of New Jersey, have concluded that a unique, numerical device identifier is *not* personally identifiable information under the statute. *Yershov* does not address these contrary decisions.

Further, in the 2015 case *Ellis v. Cartoon Network, Inc.*, the Eleventh Circuit adopted a narrower reading of "subscriber," requiring more of a "commitment" than that which arises from downloading a free app. *Yershov* distinguished the process associated with downloading and installing the apps in the *Ellis* case, but the *Yershov* and *Ellis* courts' diverging conclusions could indicate a more fundamental disagreement about what it means to download and use free software.

Yershov shows the continuing split among courts interpreting the scope of the VPPA. As a result, B2C website operators and mobile app developers that deal with video and audio materials will want to continue to monitor VPPA case law developments and to seek to identify and address associated legal risks.

APP DEVELOPER PREVAILS IN CLASS ACTION LAWSUIT CHALLENGING SHIFT TO NEW BUSINESS MODEL

By Claudia Maria Vetesi and John Delaney

If you make available a service through a free app, and you subsequently decide to migrate users of that app to a paid subscription model, that shouldn't create any problems, right?

Well, app developer LogMeIn did just that and became the target of a class action lawsuit filed in the Eastern District of California. Although the claims against LogMeIn were recently dismissed, the case, *Handy v. LogMeIn, Inc.*, highlights the potential legal risks in seeking to transition app customers from a "no charge" (or a "one-time only charge") business model to another business model, especially where the new business model will require those customers to pay ongoing subscription fees.

LOGMEIN'S PRODUCTS

LogMeIn made available a free app, LogMeIn Free, which allowed users to use a laptop or desktop computer to remotely access a separate desktop computer. The company also offered, for $29.99, a second app, Ignition, which provided the same remote access but from a tablet or smartphone.

In 2014, LogMeIn notified its customers that it would no longer offer LogMeIn Free and that it was planning to migrate all users of that app and the Ignition app to a paid subscription service, which offered a few extra features. The plaintiff—a user of LogMeIn Free and a purchaser of Ignition—brought suit under California's False Advertising Law (FAL) and Unfair Competition Law (UCL), alleging that the company had failed to properly notify users that it would discontinue these products and that, had he known LogMeIn would do so, he would not have purchased Ignition.

LogMeIn filed a motion to dismiss the plaintiff's claims and a motion for summary judgment. Because the court considered evidence outside the pleadings, it applied summary judgment standards and ruled in favor of LogMeIn.

FAILURE TO IDENTIFY ANY AFFIRMATIVE MISREPRESENTATION

The plaintiff claimed the following: (1) LogMeIn had misled consumers to believe that LogMeIn Free and Ignition apps were both being discontinued and that, in order to continue to receive the services provided through these apps, users had to pay for an annual subscription; and (2) LogMeIn had led users to believe that the free app and the paid subscription were "companion services" and, as such, had failed to inform users that the discontinuation of the free app would make the subscription app less valuable. The court rejected both theories.

First, the court held that LogMeIn had not misrepresented its intention to discontinue its free app and the Ignition product. LogMeIn explained its migration plan and offered consumers a six-month free subscription to the new subscription-based service. It further explained that, regardless of whether users accepted the complementary subscription, they could continue to use Ignition until it was discontinued. This is exactly what the plaintiff did: He continued to use the Ignition product throughout 2014 and 2015. Because the plaintiff was not "tricked" by LogMeIn's statement and did not buy the new subscription-based product because of any alleged misrepresentation, he could not base a claim on LogMeIn's statement of its migration plan. The court noted: "While [the plaintiff] may be outraged by what he feels occurred to others, the Court is not clear why he believed that this outrage makes him aggrieved such that he can vindicate this grievance in this litigation."

Second, the court held that the plaintiff failed to show that the free app and Ignition were "companion services" such that Ignition was less valuable without the free app. It noted that the plaintiff used the free app for more than a year before buying Ignition and then used Ignition for more than a year after the free app had been discontinued. The products, therefore, were not dependent on one another.

> Migrating users off of a free app or a "one-time only charge" app to a paid subscription model can spark unwanted and costly litigation.

Further, the court noted that, prior to receiving access to the LogMeIn Free app, the plaintiff and other customers had been required to "click accept" the terms and conditions governing use of that app and the Ignition app and, in such terms and conditions, LogMeIn had made clear that it reserved "the right to modify or discontinue" either LogMeIn Free or Ignition "for any reason or no reason," thereby undercutting the plaintiff's position that use of one was dependent on the other.

OBSERVATIONS

App developers (and other companies, for that matter) should take note that, even though LogMeIn ultimately prevailed, migrating users off of a free app or a "one-time only charge" app to a paid subscription model can spark unwanted and costly litigation, no matter how baseless that litigation might be; accordingly, app developers will want to proceed with caution and ideally consult experienced counsel before undertaking such an initiative.

That being said, the *Handy* decision highlights some of the challenges that a plaintiff will have in pursuing any such litigation. As the *Handy* plaintiff learned, fraud-based claims under the FAL and UCL are subject to heightened pleading requirements. Moreover, plaintiffs must allege reliance on specific statements and injury in fact as a result. Further, courts are increasingly dismissing claims that fail to allege such individualized reliance and injury.

Finally, *Handy* shows how a carefully drafted set of terms and conditions governing app usage can help to bolster an app developer's defenses to FAL, UCL and other claims arising out of a shift to a new business model. Such terms and conditions of use ideally should provide notice to users that the app (including any associated services) may be modified or discontinued, and that the app developer reserves the right to charge fees or to increase fees in connection with the app. Moreover, as in *Handy*, app developers can further strengthen the impact in litigation of an app's terms and conditions of use by requiring customers to affirm consent to such terms and conditions.

EUROPE'S RIGHT TO BE FORGOTTEN SPREADS TO ASIA

By Suhna Pierce and Adam Fleisher

In May 2014, in a decision attracting worldwide attention, the European Court of Justice (ECJ) held that a European individual's privacy rights include the "right to be forgotten," requiring Internet search engine providers to honor an individual's request to remove certain search results relating to him or her. Specifically, individuals may request deletion of links to information that is "inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes for which they were processed and in the light of the time that has elapsed."

Since the ECJ's 2014 decision, initiatives to curtail the Internet's long memory about individuals' histories have arisen in other continents. In Asia, South Korea has recently embraced a limited form of the right to be forgotten, while a court in China struggled with whether to recognize the right.

South Korea's Guidelines on Requests for Access Restrictions on Internet Self-Postings

As of June 2016, website operators and Internet search engine providers in South Korea are expected to voluntarily cooperate with guidelines issued by the Korea Communications Commission (KCC) on a form of the right to be forgotten. The KCC released the non-binding "Guidelines on Requests for Access Restrictions on Internet Self-Postings" on April 29, 2016, in response to intense interest in the matter within the country following the ECJ ruling. Operators of websites with user-contributed content and operators of web search engines may receive requests to remove or exclude information relating to individuals.

The KCC indicated its intent to strike a balance in the guidelines between protecting an individual's privacy rights and protecting freedom of expression. The guidelines are meant to address a gap that is not covered by existing remedies (e.g., under copyright law for unlawful reproduction of information, the Press Arbitration Law for erroneous reporting or the Information Network Act for posts infringing a third party's rights). The specific concern that the guidelines seek to address is the situation where an individual has "lost control" over content that he or she posted to an Internet site ("self-postings"), such as when the user of a service has canceled his or her membership to the service but the content remains available on the service.

Under the guidelines, an individual who would like to remove online self-postings should first attempt to delete the content. If he or she is unable to delete the content, the individual may request that the site administrator restrict access to the materials. The request to remove or exclude content should include the URL of the material to be removed, proof that the requestor posted the content and the reason for removing the content. The site operator may request additional information if the request contains insufficient proof to determine that the requestor posted the content, and the site operator may thereafter deny the request if the additional information provided is still insufficient.

The plaintiff sought a ruling that a Chinese individual's privacy rights include a right to be forgotten, similar to that of European individuals.

Upon removal of the content, the site operator should inform third parties of the removal by publishing a note in place of the removed content that access to the content has been restricted. A third party may appeal the removal of content by providing the website operator with both evidence that he or she authored the content, and a reason for reinstating it. Additionally, a requestor who misrepresents another person's post as his or her own in order to have it removed may be subject to civil and criminal penalties.

The individual may also request Internet search engine operators to exclude the content from search results, although it is unclear whether the individual must have originally published the content to be excluded. As a result, the rights afforded to individuals under the KCC guidelines appear to be more limited in scope than the broad rights recognized under the ECJ's decision.

The KCC's press release and a copy of the guidelines are available (in Korean) and can be found here.

China Rejects the Right to Be Forgotten, at Least for Now

In contrast to the formal—albeit voluntary—regime that has just taken effect in South Korea, the right to be forgotten does not yet appear to be recognized in China. This is so, notwithstanding the recent efforts of a plaintiff seeking to convince a Chinese court to import the right from Europe into China. Indeed, a summary of the case posted by the Haidian District People's Court in Beijing expressly acknowledges the ECJ's May 2014 ruling.

The case involved a plaintiff seeking to compel a search engine to remove results that related to him. In its ruling, the court concluded the plaintiff had no right to be forgotten. The plaintiff, Ren Jiayu, sued the search engine Baidu after a search on his name pulled—in the "related searches" section on the bottom of the results page—various references to Ren and Taoshi Education Company. Ren was apparently associated with this company in the past, but the company was in ill repute ("many people believed that Taoshi Education was a dishonest company, with some going so far as to claim it was an evil cult," explained the Beijing court of first instance in its ruling, according to a recent report on these developments). Ren's employment with Beijing Daoyaxuan Commercial Trading Company Limited was terminated as a result of the association, and he then sued Baidu seeking lost wages and the elimination of a number of keywords from search results for "Ren Jiayu," including "Taoshi Education Ren Jiayu."

In other words, Ren sought a ruling that a Chinese individual's privacy rights include a right to be forgotten, similar to that of European individuals, which would require Baidu to honor his request to remove search results information relating to him.

Ren argued that the "related searches" terms should be removed in part because he had no prior relationship with the offending company. The court, however, found that he did, and thus concluded that there was no infringement of Ren's right to his reputation. The court also rejected any claim that Baidu had infringed on Ren's right to his name. Then, the court turned to whether there could be a new right to be forgotten within the framework of the "general right of personhood" under Chinese law.

The court first noted that, even though there was a right to be forgotten in other countries, including countries of the European Union, that jurisprudence would not inform the court's decision.

The court then identified three criteria for the right to be forgotten under Chinese law: the personal interest at issue must (1) encompass a right not already categorized; (2) be legitimate; and (3) require the protection of law.

The court acknowledged that Ren had an interest in having the information "forgotten"—it had an adverse impact on his employment prospects—but this interest was not "legitimate and requiring the protection of law." As the court put it, the search results "relat[e] to very recent events, and [Ren] continues to work in the business administration education profession. This information happens to form a portion of his professional history, and his current individual professional credibility is both directly relevant and of ongoing concern."

In short, while the Chinese court appears to have concluded that there is no such thing as a right to be forgotten, the case could also be read to suggest that there was no such right based on the facts of this case but that it is plausible that some other individual's interest in having search results removed could be found to be legitimate and require the protection of the law.

An article (in English) describing the case and providing links to the rulings (in Chinese) can be found here.

Although the right to be forgotten has not yet taken force in China, the door remains open for further efforts to establish the right. And although the right currently exists only in non-binding guidance in South Korea, this guidance highlights the growing interest in Asia in what could ultimately become one of Europe's hottest exports.

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**.