Volume 6, Issue 2, May 2015

# SOCIALLY AWARE

## THE SOCIAL MEDIA LAW UPDATE

THE BURTON AWARDS FOR THE PURSUIT OF PERFECTION
2011 BEST LAW FIRM NEWSLETTER

IN THIS ISSUE



EDITORS

John F. Delaney
Aaron P. Rubin

CONTRIBUTORS

Patrick J. Bernhardt
Libby J. Greismann
J. Alexander Lawrence
Christine E. Lyon
Susan McLean
Julie O'Neill
Aaron P. Rubin
Chanwoo Park
Mercedes Samavi
Daniel A. Zlatnik

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 a recent decision in Virginia protecting the anonymity of Yelp users; we examine the FTC's much anticipated report, "Internet of Things: Privacy & Security in a Connected World;" we explore the major social media platforms' approaches to handling deceased users' accounts; we highlight a recent CJEU case holding that extracting large amounts of data from public websites—commonly known as "web scraping"—may violate website's terms of use; we highlight the first-ever award of "any damages" for fraudulent DMCA takedowns; we drill down on important precedents that are defining the multi-channel programming distribution industry; and we take a look at cross-device tracking in interest-based advertising.

All this—plus an infographic featuring some intriguing online dating statistics.

# COURT PROTECTS ANONYMITY OF YELP USERS

**By Chanwoo Park and J. Alexander Lawrence**

Virginia's highest court recently held that Yelp could not be forced to turn over the identities of anonymous online reviewers that a Virginia carpet-cleaning owner claimed tarnished his business.

In the summer of 2012, Joseph Hadeed, owner of Hadeed Carpet Cleaning, sued seven anonymous Yelp reviewers after receiving a series of critical reviews. Hadeed alleged that the reviewers were competitors masking themselves as Hadeed's customers and that his sales tanked after the reviews were posted. Hadeed sued the reviewers as John Doe defendants for defamation and then subpoenaed Yelp, demanding that it reveal the reviewers' identities.

Yelp argued that, without any proof that the reviewers were not Hadeed's customers, the reviewers had a First Amendment right to post anonymously.

A Virginia trial court and the Court of Appeals sided with Hadeed, ordering Yelp to turn over the reviewers' identities and holding it in contempt when it did not. But in April 2015, the Virginia Supreme Court vacated the lower court decisions on procedural grounds. Because Virginia's legislature did not give Virginia's state courts subpoena power over non-resident non-parties, the Supreme Court concluded, the Virginia trial court could not order the California-headquartered Yelp to produce documents located in California for Hadeed's defamation action in Virginia.

Although the decision was a victory for Yelp, it was a narrow one, resting on procedural grounds. The Virginia Supreme Court did not address the broader First Amendment argument about anonymous posting and noted that it wouldn't quash the subpoena because Hadeed could still try to enforce it under California law.

After the ruling, Yelp's senior director of litigation, Aaron Schur, posted a statement on the company's blog stating that, if Hadeed pursued the subpoena in California, Yelp would "continue to fight for the rights of these reviewers under the reasonable standards that California courts, and the First Amendment, require (standards we pushed the Virginia courts to adopt)." Schur added, "Fortunately the right to speak under a pseudonym is constitutionally protected and has long been recognized for the important information it allows individuals to contribute to public discourse."

**Yelp argued that its reviewers have a First Amendment right to post anonymously.**

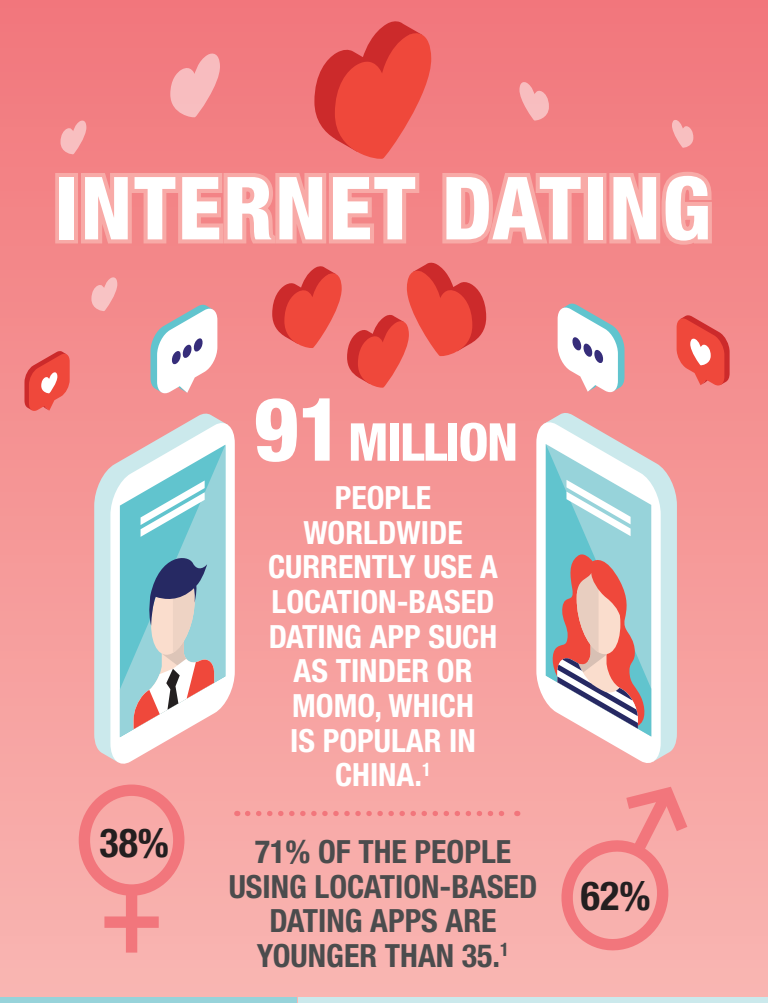
In 2009, a California law took effect, allowing anonymous Internet speakers whose identity is sought under a subpoena in California in connection with a lawsuit filed in another state to challenge the subpoena and recover attorneys' fees if they are successful. In his Yelp post, Schur added that Hadeed's case "highlights the need for stronger online free speech protection in Virginia and across the country."

Had Hadeed sought to enforce the subpoena in California, the result may have been the same but possibly on different grounds. In California, where Yelp and many other social media companies are headquartered, the company would have been subject to a court's subpoena power. Still, Yelp may have been protected from having to disclose its users' identities. California courts have offered protections for anonymous speech under the First Amendment to the U.S. Constitution and the state constitutional right of privacy.

Nevertheless, there is no uniform rule as to whether companies must reveal identifying information of their anonymous users. In 2013, in *Chevron v. Danziger*, federal Magistrate Judge Nathanael M. Cousins of the Northern District of California concluded that Chevron's subpoenas seeking identifying information of non-party Gmail and Yahoo Mail users were enforceable against Google and Yahoo, respectively, because the subpoenas did not seek expressive activity and because there is no privacy interest in subscriber and user information associated with email addresses.

On the other hand, in March 2015, Magistrate Judge Laurel Beeler of the same court held, in *Music Group Macao Commercial Offshore Ltd. v. Does*, that the plaintiffs could not compel nonparty Twitter to reveal the identifying information of its anonymous users, who, as in the Hadeed case, were Doe defendants. Music Group Macao sued the Doe defendants in Washington federal court for anonymously tweeting disparaging remarks about the company, its employees, and its CEO. After the Washington court ruled that the plaintiffs could obtain the identifying information from Twitter, the plaintiffs sought to enforce the subpoena in California. Magistrate Judge Bheeler concluded that the Doe defendants' First Amendment rights to speak anonymously outweighed the plaintiffs' need for the requested information, citing familiar concerns that forcing Twitter to disclose the speakers' identities would unduly chill protected speech.

Courts in other jurisdictions have imposed a range of evidentiary




burdens on plaintiffs seeking the disclosure of anonymous Internet speakers. For example, federal courts in Connecticut and New York have required plaintiffs to make a prima facie showing of their claims before requiring internet service providers (ISPs) to disclose anonymous defendants' identities. A federal court in Washington found that a higher standard should apply when a subpoena seeks the identity of an Internet user who is not a party to the litigation. The Delaware Supreme Court has applied an even higher standard, expressing concern "that setting the standard too low will chill potential posters from exercising their First Amendment right to speak anonymously."

These cases show that courts are continuing to grapple with social media as a platform for expressive activity. Although Yelp and Twitter were protected from having to disclose their anonymous users' identities in these two recent cases, this area of law remains unsettled, and companies with social media presence should be familiar with the free speech and privacy law in the states where they conduct business and monitor courts' treatment of these evolving issues.

# FTC ISSUES LANDMARK REPORT ON INTERNET OF THINGS

**By Libby J. Greismann and Christine E. Lyon**

The Federal Trade Commission (FTC) has released its much anticipated report on the Internet of Things ("IoT")—a topic that has been top-of-mind for many companies. The FTC's report, "Internet of Things: Privacy & Security in a Connected World" (the "Report"), discusses the benefits and risks associated with IoT, and addresses the privacy and data security measures the FTC recommends for consumer-facing IoT products and services (The FTC's discussion of IoT within the report, consistent with the FTC's jurisdiction, is limited to such devices that are sold to or used by consumers, and not devices sold in a business-to-business context or broader machine-to-machine communications). While the Report is not legally binding, it provides a strong and valuable indication of the positions that the FTC may take in enforcement actions related to IoT.

## WHAT IS THE INTERNET OF THINGS?

According to the FTC, IoT refers to "things, such as devices or sensors—other than computers, smartphones, or tablets—that connect, communicate or transmit information with or between each other through the Internet."

## FTC RECOGNIZES BENEFITS AND RISKS OF IOT

The Report acknowledges that Internet-connected devices offer numerous benefits, many of which remain untapped. In the health arena, connected medical devices allow patients to more efficiently communicate with their physicians to manage their medical conditions. In the home, smart meters enable energy providers to analyze consumer energy use, identify issues with home appliances and enable consumers to be more energy-conscious. On the road, sensors on a car can notify drivers of dangerous road conditions, and software updates can occur wirelessly. And these applications are just the beginning.

> The FTC asserts that "inadequate security presents the greatest risk of actual consumer harm in the Internet of Things."

On the flip side, however, the FTC cautions that IoT may present a variety of potential security vulnerabilities that could be exploited to harm consumers. First, as with computers, a lack of security could enable unauthorized access and misuse of personal information. This risk is heightened in the IoT world by the plethora of devices to be connected and secured. Second, security vulnerabilities in a particular device may facilitate attacks on the consumer's network to which it is connected, or enable attacks on other systems. Third, the FTC notes that IoT may present a heightened risk of harm to personal safety. For example, the Report describes an account of how it may be possible to hack remotely into a connected medical device and change its settings, impeding its therapeutic function.

According to the FTC, these risks are exacerbated by the fact that companies entering the IoT market may not have experience in dealing with security issues, or may be creating inexpensive devices for which it may be difficult or impossible to apply a patch for a security bug.

## SECURITY

In light of these increased risks, the FTC asserts that "inadequate security presents the greatest risk of actual consumer harm in the Internet of Things." As such, it recommends that companies focus on security when developing connected devices. The FTC acknowledged that what constitutes reasonable security for a given device will depend on a number of factors, including the amount and sensitivity of data collected, and the costs of remedying the security vulnerabilities. However, the staff did offer approaches that it encourages companies to adopt when developing their products:

- Building security into their devices at the outset, by conducting an initial privacy or security risk assessment, considering how to minimize the data collected and retained, and testing security measures before launching the product.
- Training all employees about good security, and ensuring that security issues are addressed at the appropriate levels of responsibility within the organization.
- Retaining service providers that are capable of maintaining reasonable security and providing reasonable oversight.
- Implementing a defense-in-depth approach for systems that involve significant risks, considering security measures at several levels.
- Imposing reasonable access control measures to limit the ability of an unauthorized person to access a consumer's device, data or network.
- Continuing to monitor products throughout the life cycle and, to the extent possible, patch known vulnerabilities.

In sum, devices that collect sensitive information, present physical security or safety risks (such as door locks, ovens or medical devices), or connect to other devices or networks in a manner that would enable unauthorized access to those devices, may require heightened consideration of security measures.

## DATA MINIMIZATION

The Report emphasizes the FTC's view that companies should reasonably limit their collection and retention of consumer data, including in the IoT context. The FTC believes that these practices, known as data minimization, will help guard against two privacy-related risks: first, larger data stores present a more attractive target for data thieves; and second, if a company collects and retains large amounts of data, there is an increased risk that the data will be used in a way that departs from consumers' reasonable expectations.

At the same time, the Report acknowledges concerns that data minimization requirements may curtail innovative uses of data. Accordingly, the FTC proposes a "flexible" approach to data minimization that gives companies a variety of options: they can decide not to collect data at all, collect only the fields of data necessary to the product or service being offered, collect data that is

less sensitive, or de-identify the data they collect. The FTC also suggests that if none of these options works, a company can seek consumers' consent for collecting additional, unexpected data.

### NOTICE AND CHOICE

The FTC acknowledges that notifying consumers of privacy principles and offering them a way to meaningfully choose privacy settings may be more difficult in the context of connected devices, which may not have a screen with which to communicate with consumers. However, the report makes clear that the FTC does not believe it will be sufficient for IoT companies to simply have a privacy policy available on their websites, and expect consumers to find that policy. Rather, the FTC recommends that a company find ways to present meaningful privacy notices and choices to the consumer, including in the set-up or purchase of the product itself. The Report suggests creative solutions to this issue, including:

- Offering video tutorials to guide consumers through privacy settings.
- Affixing a QR code that, when scanned, would take the consumer to a website with information about privacy practices.
- Offering a set-up wizard that provides information about privacy practices.
- Allowing users to configure devices, such as home appliances, so that they receive information through emails or texts.
- Creating a user experience "hub" that stores data locally and learns a consumer's privacy preferences based on prior behavior.

Companies may also want to consider using a combination of approaches. Of course, whatever approach a company decides to take, the FTC expects the privacy choices to be clear and prominent, and not buried within lengthy documents.

### LEGISLATION

Last but not least, the FTC reiterated its recommendation for Congress to enact strong, flexible, and technology-neutral legislation to strengthen the Commission's existing data security enforcement tools, and require companies to notify consumers when there is a security breach.

### CONCLUSION

As the FTC describes, "in the future, the Internet of Things is likely to meld the virtual and physical worlds together in ways that are currently difficult to comprehend." As a result, companies should consider guidance offered by the FTC and other regulators, and evaluate what steps they can take to mitigate those risks in the privacy and data security context.

## WHO WILL UPDATE MY STATUS WHEN I'M DEAD?: THE BIGGEST SOCIAL MEDIA PLATFORMS' POLICIES ON DECEASED-USER ACCOUNTS

**By Aaron P. Rubin**

It's often said that, when it comes to regulating technology, U.S. laws aren't up to speed. That includes U.S. trusts and estates laws, which, in many cases, do not say much about what happens to your digital assets after you die.

Unless you or your trustee lives in one of the few states that has a law that allows your executor to access your online accounts, your loved ones may have to follow the procedures set forth in social media platforms' terms of use if they want to access your account after your death.

Unless you or your trustee lives in one of the few states that, like Delaware, has a law that allows your executor to access your online accounts, your loved ones may have to follow the procedures set forth in social media platforms' terms of use if they want to access your account after your death. (Alternatively, a deceased social-media-account holder's survivors could seek a court order granting them access to your social media accounts, but it's a lengthy and not-always-successful process.)

The fluid nature of the major social media platforms' approach to handling deceased users' accounts is illustrated by Facebook, which recently changed its policy to afford users more post-mortem control over their pages. The recent press coverage of Facebook's policy piqued our curiosity regarding how the major social media platforms address this issue. Below we summarize Facebook's, Twitter's, Instagram's, Pinterest's, LinkedIn's and Google's (including Google companies YouTube's and Blogger's) policies regarding management of deceased users' accounts.

## FACEBOOK: ALLOWS USERS, WHILE THEY'RE ALIVE, TO DESIGNATE A "LEGACY CONTACT," OR ELECT TO HAVE THE ACCOUNT DELETED AFTER THEY'VE DIED

Facebook recently changed its terms of service to allow the platform's U.S. users to elect to have their accounts permanently deleted after they die, or to select a "legacy contact"— a family member or friend to whom Facebook will accord limited management of the user's Facebook account after the user dies. Once a friend of the deceased user completes an online form notifying Facebook of the user's death, Facebook will add the tagline "Remembering" over the user's name and notify the legacy contact. The legacy contact may then: (1) download the photos and other information that the deceased shared on Facebook (if the deceased indicated that he or she would like to give the legacy contact that permission); (2) "write a post to display at the top of the memorialized Timeline (for example, to announce a memorial service or share a special message)"; (3) update the profile photo and cover photo; and (4) accept new friend requests on the deceased's behalf.

The legacy contact will not be able to access the deceased's private messages or login as the deceased.

Step-by-step instructions on how to designate a Facebook legacy contact are available here.

## TWITTER: OFFERS ONLY POSSIBLE ACCOUNT DELETION AT THE REQUEST OF THE DECEASED'S LAWFUL REPRESENTATIVE OR IMMEDIATE FAMILY MEMBER

Twitter's terms of use specifically provide that the company is "unable to provide account access to anyone regardless of his or her relationship to the deceased." Twitter will, however, "work with a person authorized to act on the behalf of the estate or with a verified immediate family member of the deceased to have an account deactivated."

To fulfill this request, the company requires significant proof of the requester's relationship with the deceased, including a death certificate.

## INSTAGRAM: OFFERS TO MEMORIALIZE ACCOUNTS UPON PROOF OF DEATH; WILL ONLY REMOVE AN ACCOUNT AT FAMILY'S REQUEST

Instagram's policy says that the company will heed a request to memorialize a deceased person's account from anyone who provides proof of the death, such as a link to an obituary or a news article. The company will not provide anyone with login information for memorialized accounts. For Instagram to remove a deceased person's account, an immediate family member must make the request. Instagram's policy requires that removal requesters prove their status as a member of the deceased's immediate family by providing documents such as the deceased's birth or death certificate, or "proof of authority under local law that you are the lawful representative of the deceased person, or his/her estate."

## PINTEREST: OFFERS ONLY ACCOUNT DELETION AT THE REQUEST OF A FAMILY MEMBER

Pinterest's terms of use also state that, in the interest of the platform's users' privacy, the company won't give out login information, but will "deactivate a deceased person's account if a family member gets in touch with us." True to Pinterest's homey image, the company will accept less formal documentation of the requester's relationship with the deceased, including a "family tree."

Of the terms of use that we examined, Pinterest's were the only ones to offer condolences, stating, "We're so very sorry to hear about the loss of your loved one."

## LINKEDIN: OFFERS ONLY ACCOUNT DELETION AT THE REQUEST OF ANYONE WITH A RELATIONSHIP TO THE DECEASED AND A LINK TO THE DECEASED'S OBITUARY

LinkedIn's terms of use state that the company will close the account and remove the profile of "a colleague, classmate, or loved one who has passed away" if the requester provides certain basic information and a link to the deceased's obituary.

## GOOGLE+, YOUTUBE, BLOGGER: ALLOWS A USER, WHILE HE OR SHE IS ALIVE, TO DESIGNATE UP TO 10 PEOPLE WITH WHOM GOOGLE WILL SHARE THE USER'S DATA AFTER THE USER HAS DIED

In keeping with its reputation as an extremely progressive company, Google since 2013 has allowed its social media platforms' users a good measure of post-mortem control over their digital assets. Under Google's terms of use, which have been in place for the last couple of years, a user of +1s, Blogger, Contacts and Circles, Drive, Gmail, Google+ Profiles, Pages and Streams, Picasa Web Albums, Google Voice and YouTube may select a time period of account inactivity—three, six, nine or 12 months—after which Google will fulfill the user's wishes for the post-mortem disposition of his or her account (after first warning the user by sending a text message to his or her cellphone and an email to a secondary address that the user provided). At that point, Google will notify "up to 10 trusted friends" that the user's account is inactive, and—if the user so chooses—share his or her data with all or some of those people.

Users can also elect to have Google delete their accounts or set up an auto-response to all incoming messages once a user's account becomes inactive.

To instruct Google on what you'd like the company to do with your Google accounts and the data in them after you've died, go to the Account Settings page of the Google platform that you use, scroll down to the Account Tools subheading, and click on Inactive Account Manager.

# DATA FOR THE TAKING: USING WEBSITE TERMS AND CONDITIONS TO COMBAT WEB SCRAPING

**By Susan McLean and Mercedes Samavi**

Is it stealing to take data without permission from a public website, or is it simply making use of resources that are made available to you? "Web scraping" or "screen scraping" is the practice of extracting large amounts of data from public websites using bots.

A recent case in the European Court of Justice (CJEU) has focused attention both on the intellectual property infringement aspects of scraping practices and on the potential for website owners to use their sites' contractual terms and conditions to combat the scrapers.

Scraping is not new, but it has become increasingly widespread in recent years, fuelled by the rise in big data analytics and the popularity of price comparison websites. Indeed, in 2013, scraping accounted for 18% of site visitors and 23% of all Internet traffic. Scraping is not inherently bad: it can have legitimate uses, spur innovation and give companies with limited resources access to large amounts of data. Unsurprisingly, however, many website operators do not like it. Not only are operators keen to protect their proprietary rights, but repeated scraping can also take a heavy toll on websites by using up bandwidth and leading to network crashes.

In the U.S., website operators have asserted various claims against scrapers, including copyright claims, trespass to chattels claims and contract-based claims alleging that scrapers violated their website terms of use. In the EU, operators have tended to rely on intellectual property infringement claims against scrapers, but there has been little case law to provide guidance.

In January 2015, however, in a much anticipated decision, the CJEU held that where a website operator cannot establish intellectual property rights in its database, an operator may still be able to rely on its website terms and conditions to prohibit scraping. This ruling may impact an increasing number of companies whose business models rely on mining data from websites' and social media platforms without permission. On the other hand, it will be viewed positively by those data-rich businesses keen to protect and/or monetize their data.

## RYANAIR LTD V PR AVIATION

The CJEU case involved PR Aviation, which operates a price-comparison website for low-cost airlines. Consumers can book a flight on the website and PR Aviation receives a commission. The website relies on information obtained by screen scraping publicly available data from the websites of low cost airlines, including data from Ryanair's website.

Ryanair sued the defendant for infringement of database rights under the Database Directive (96/9/EC), and breach of its website terms and conditions. It sought an order against PR Aviation to refrain from any further infringement on pain of a financial penalty and for PR Aviation to pay damages.

## WHAT ARE DATABASE RIGHTS?

Database rights are a form of unregistered intellectual property rights introduced by the Database Directive in 1996 and implemented into national law across the European Union.

Is it stealing to take data without permission from a public website, or is it simply making use of resources that are made available to you?

The aim of the Database Directive was to harmonize the rules that applied to copyright protection of databases across the EU, safeguard the investment of database makers and secure the legitimate interests of database users. In essence, the Directive sought to create a legal framework appropriate to the use of databases in the information age. It did so by ensuring copyright protection for those elements of databases possessing protectable expression and introducing a new form of *"sui generis"* protection for those elements of databases which are not "original" in the sense of being the author's own intellectual creation.

Accordingly, the Database Directive provides two forms of protection. Article 3(1) establishes the first of these rights: "*databases which by reason of the selection or arrangement of their contents, constitute the author's own intellectual creation shall be*

*protected as such by copyright*". The second form of protection (established by Article 7) provides protection where there *"has been qualitatively and/or quantitatively a substantial investment in either the obtaining, verification or presentation of the contents [of a database]"*.

Importantly, the Database Directive includes certain limited exceptions to the rights created. In particular, Article 6 allows lawful users to make a copy of a copyright-protected database without consent where it is necessary to do so in order to access its contents. Further, Article 8 permits lawful users of a publicly available database to extract and/or reuse insubstantial parts of its contents, as long as this use does not conflict with normal exploitation of the database or unreasonably prejudice the legitimate interests of the database's author.

## DUTCH SUPREME COURT

The Ryanair dispute ended up in the Dutch Supreme Court where PR Aviation successfully argued that Ryanair could not rely on copyright protection because Ryanair's database was not sufficiently original to attract copyright protection, and also that there had been insufficient investment by Ryanair, in compiling its database, for it to claim the *sui generis* right.

However, the court still faced the question whether Ryanair could assert a claim that PR Aviation had breached Ryanair's website terms and conditions by scraping and re-using data from the Ryanair site. Significantly, Ryanair's website terms and conditions contain the following express prohibition on the use of screen scraping: *"The use of automated systems or software to extract data from this website or www.bookryanair.com for commercial purposes ('screen scraping') is prohibited unless the third party has directly concluded a written license agreement with Ryanair which permits access to Ryanair's price, flight and timetable information for the sole purpose of price comparison."*

**In a much anticipated decision, the European Court of Justice (CJEU) has held that where a website operator cannot establish intellectual property rights in its database, an operator may still be able to rely on its website terms and conditions to prohibit scraping.**

Ryanair sought to enforce this term. PR Aviation argued that the prohibition against screen scraping was not enforceable because, under Article 15 of the Database Directive, any contractual provisions which are contrary to Articles 6 and 8 are rendered null and void. The Dutch Supreme Court was unsure whether Article 15 of the Directive applied to a database which did not attract copyright protection or the *sui generis* right and therefore it sought a preliminary ruling from the CJEU.

## CJEU DECISION

In a logical ruling, the CJEU ruled that the limitations on rights introduced by the Database Directive do not apply to databases that are not protected by the Directive. Accordingly, Articles 6, 8 and 15 of the Database Directive do not preclude a website operator from laying down contractual limits on the use of a database, without prejudice to applicable national law.

The case has now been sent back to the Dutch courts, which must decide on the enforceability of the Ryanair website terms and conditions.

For a website owner, it is not simply a question of prohibiting scraping in its terms and conditions; an operator also needs to ensure that those terms and conditions are enforceable. We have written before about the issues involved, particularly in Europe, in ensuring that online terms are deemed fair and reasonable.

Ideally, a website operator would require any user of its site to accept the website terms and conditions before allowing the user to access the website. However, the majority of sites are reluctant to enforce this rule because it is not considered user-friendly. It is therefore more common to ensure that a link to the terms is displayed prominently on the site. The problem with this method is that there is no active acceptance of the terms (e.g., clicking a box). As a result, there is a risk that the website owner will be unable to demonstrate that there is a contract in place with the user. This is a question for national law, as indicated in this case.

There is no binding case law on the issue in the UK. Unfortunately, although the issue was touched on in the recent high-profile *Newspaper Licensing Agency v Meltwater [2011] EWCA Civ 890*, the Court of Appeal did not consider whether an end-user was bound by the website terms of use because, given the nature of the case, it said that it was unnecessary "to enter into that controversy."

Lastly, the *Ryanair* judgment does not answer the question of whether a screenscraper would ever be able to rely on the lawful use exceptions set out in Article 6 or 8 of the Database Directive if the database owner were able to establish copyright protection or the *sui generis* right in the database.

## OTHER CLAIMS

It is worth pointing out that, in addition to intellectual property rights infringement and contract breach claims, website owners may have other legal arguments against scraping. For example, as in the U.S., in the UK, a website operator may try to bring a claim for trespass to chattels, a common law tort. In addition, an operator may seek to rely on the Computer Misuse Act 1990 which prohibits unauthorized access to, or modification of, computer material. To date, as with database rights, neither of these arguments has been tested in the UK courts in connection with web scraping. (Similar legislation, however, has formed the basis of claims elsewhere, for example, in the U.S., as described in our previous alert, "Data for the Taking: Using the Computer Fraud and Abuse Act to Combat Web Scraping.")

Of course, when dealing with scraped data, issues of privacy and security loom large and web scrapers and users of scraped data will also need to tread extremely carefully in order to avoid problems under applicable privacy laws. For a detailed discussion on privacy and big data, see our previous Alert.

## CONCLUSION

The CJEU's *Ryanair* decision appears to give a rather contrary result—in certain circumstances, a database owner may have broader, albeit contractual, rights to prevent scraping if it does not actually have proprietary rights in the database. However, in any event, in light of this decision, website owners based in the EU may be encouraged to amend their website terms and conditions to expressly prohibit screen-scraping in order to try to protect their valuable data.

Whether the impact of this decision will truly disrupt those companies with business models that rely on the use of data mined from websites and social media platforms remains to be seen. Certainly, any business that carries out screen-scraping activities should consider where it sources its data from and identify whether such data are bound by contractual limitations or other restrictions. It can then make a reasoned decision on whether or not it should approach the database owner for a commercial license to ensure that the data keeps flowing.

# FIRST-EVER AWARD OF "ANY DAMAGES" FOR FRAUDULENT DMCA TAKEDOWNS UNDER SECTION 512(F)

**By Daniel A. Zlatnik and Aaron P. Rubin**

Under section 512(f) of the Digital Millennium Copyright Act (DMCA), copyright owners are liable for "any damages" stemming from knowingly false accusations of infringement that result in removal of the accused online material. Section 512(f) aims to deter abuse of the DMCA requirement that service providers process takedown requests from purported copyright owners, but such abuses remain rampant. (e.g., as reported here and here.) In fact, until the March 2, 2015, decision in *Automattic Inc. v. Steiner* (adopting magistrate's earlier recommendation), no court had awarded damages under section 512(f).

The case concerned a blog by Oliver Hotham, who had contacted a group called "Straight Pride UK," identifying himself as "a student and freelance journalist" and submitting a list of questions. Nick Steiner responded by identifying himself as the "Press Officer" for Straight Pride UK and providing a PDF file titled "Press Statement – Oliver Hotham.pdf." The press statement laid out Straight Pride UK's opposition to "everyone [in the UK] being forced to accept homosexuals" and stated its mission of ensuring "that heterosexuals are allowed to have a voice and speak out against being oppressed." Hotham posted material from the press statement on his blog.

Steiner, apparently displeased with the subsequent negative attention, sent an email to Automattic, Inc., the blog's host, invoking section 512(f). Steiner claimed to hold copyright in the posted material and requested that Automattic remove the blog post, and Automattic complied. Hotham, however, again posted material from the Press Statement to his blog, prompting Steiner to send two more removal requests by email to Automattic. Automattic denied those requests, citing their legal insufficiency. Automattic and Hotham then filed a lawsuit to recover damages related to Steiner's misrepresentation that the blog infringed his copyright.

> This was the first case resulting in a damages award under section 512(f), so the opinion is likely to serve as a road map for future courts considering such damages.

The court easily found that Steiner had violated section 512(f) because he "could not have reasonably believed that the Press Statement he sent to Hotham was protected under copyright." Following the precedent of *Lenz v. Universal Music Corp.*, the court then interpreted the statute's

specification of "any damages" to mean that damages are available, no matter how insubstantial. After requesting more detailed evidence concerning damages, the court found that Hotham and Automattic were entitled to certain types of damages.

First, based on the time he was prevented from spending on freelance articles and his expected compensation for such work, Hotham estimated the value of the time he spent on activities related to the incident, including responding to media inquiries. Hotham also requested additional damages for "lost work" due to the "significant distraction" caused by the media coverage and legal disputes. Hotham claimed a total of $960, and the court found his declaration sufficient to support that claim. But the court denied Hotham's request for reputational harm as speculative, and rejected Hotham's request for damages based on emotional distress and "chilled speech," citing the lack of authority that such damages are available under section 512(f).

Automattic was likewise successful in claiming damages of $1,860, calculated based on employee salaries and a 2,000-hour year, for time spent responding to the takedown notices and related press inquiries. The court denied Automattic's request for damages attributable to time spent by its outside public relations firm, however, because there was insufficient evidence to show how that time constituted a loss to Automattic.

The court also awarded attorneys' fees, which are expressly allowed by section 512(f). Based on comprehensive billing records submitted along with data indicating the average local billing rate for IP attorneys, the court granted the request for recovery at a rate or $418.50 per hour, for a total of $22,264 in fees.

The court's analysis is instructive in multiple ways. First, as mentioned, this was the first case resulting in a damages award under section 512(f), so the opinion is likely to serve as a road map for future courts considering such damages. Potential litigants should not read this case, however, as necessarily indicative of the magnitude of damages available in section 512(f) cases. Exposure can certainly be much greater, as demonstrated in *Online Policy Group v. Diebold, Inc.*, a case that reportedly settled for $125,000. A few factors conspired to make damages in this case minimal (a total of $25,084). Steiner's takedown notice was obviously fraudulent, so practically no resources were expended in meeting the normally demanding burden of proof. (As other commentators have noted, that same demanding burden of proof is one reason why there are not many section 512(f) cases in the first place.) Other cases may involve more protracted conflict over takedown notices and legal threats. Steiner also never appeared in his defense and therefore defaulted, which likely greatly reduced the time and expense of the lawsuit.

This case also reinforces the most crucial strategic consideration for service providers in responding to a DMCA takedown notice: as *Socially Aware* has previously explained, no damages can be awarded under section 512(f) unless the notice actually prompts the removal of the accused material. Therefore, if it ultimately wants to resist a takedown notice, a service provider can only recover the expenses of doing so if it actually removes the accused material in the first place.

On the other hand, the court applied the takedown requirement loosely in its actual assessment of damages. Steiner issued *three* purported DMCA takedown notices, but only the *first* notice resulted in actual removal of accused content. Even though Hotham and Automattic could have incurred a portion of their expenses due to the final two notices, the court did not discuss whether the takedown requirement precluded any portion of their claimed damages. While this bodes well for the availability of damages in cases involving multiple takedown notices, the analysis has questionable weight on this point. Given the absence of any opposition from the defendant, future defendants will have a strong argument that the court simply did not consider this nuance.

# WITH HIGHLY ANTICIPATED COPYRIGHT DECISION, THE AUTOHOP LITIGATION IS COMING TO A CLOSE

**By J. Alexander Lawrence**

In 2012, DISH Network announced two novel product offerings that would result in considerable backlash from the four major broadcast television networks and set in motion a three-year, wide-ranging, multi-front battle with the networks. As the dust now begins to settle, the copyright litigation has resulted in important precedents that will help define the boundaries under the Copyright Act for the multi-channel programming distribution industry.

## DISH INTRODUCES PRIMETIME ANYTIME AND AUTOHOP

On January 9, 2012, at the Consumer Electronics Show (CES) in Las Vegas, DISH unveiled its PrimeTime Anytime service. In

connection with its two-terabyte Hopper DVR, PrimeTime Anytime allows DISH subscribers, with a few pushes of a button, to copy up to eight days of ABC, NBC, CBS and Fox primetime programs. Once initiated, the service continually makes copies of the primetime lineup going forward, with the last eight days available for the subscriber.

**While Fox argued the *Aereo* decision was a "game-changer," the district court disagreed.**

About four months later, on May 10, 2012, DISH introduced AutoHop, which works in conjunction with the PrimeTime Anytime service and allows subscribers, with the single push of a button, to replay those network programs without advertisements. Viewed as a serious threat to their advertising supported revenue model, the introduction of this ad-skipping technology pushed the major networks to take action.

On May 24, 2014, the networks launched litigations. In the Central District of California, Fox, NBC and CBS, each in separate cases, filed copyright infringement complaints against DISH. *See*, *Fox Broad. Co. v. Dish Network LLC*, 2:12-cv-04529-DMG-SH (C.D. Cal.), *NBC Studios LLC v. Dish Network Corp.*, 2:12-cv-04536-DMG-SH (C.D. Cal.), and *CBS Broad. Inc. v. Dish Network Corp.*, 2:12-cv-04551-DMG-SH (C.D. Cal.). On the same day, DISH—apparently seeking the protection of the then more favorable Second Circuit authority, including *Cartoon Network LP, LLLP v. CSC Holdings, Inc.*, 536 F.3d 121 (2d Cir. 2008) (the "*Cablevision* decision")—preemptively moved for declaratory judgments against ABC and the other networks in the Southern District of New York. *See*, *Dish Network, L.L.C. v. Am. Broad. Cos., Inc.*, 1:12-cv-04155-LTS-KNF (S.D.N.Y.).

Ultimately, the cases proceeded on two tracks, with the Fox and NBC cases proceeding in California before the Honorable Dolly M. Gee, and the ABC and CBS cases proceeding in New York before the Honorable Laura Taylor Swain.

While the networks also pursued breach of contract claims arising out of their existing agreements with DISH, the focus here is on the core copyright claims. Counterparties like DISH and the networks will often agree to expand or limit their own rights under the Copyright Act depending on their own commercial interests, but the more lasting legacy of the AutoHop cases will be the copyright precedents they have established.

## DISH WINS THE EARLY ROUNDS IN CALIFORNIA

On August 22, 2012, Fox made the first move and sought a preliminary injunction against DISH's PrimeTime Anytime and AutoHop services. Fox suffered an early defeat. On November 7, 2012, the district court denied Fox's motion for preliminary injunction, finding that Fox had not established a likelihood of success on the merits of its claims with respect to those two services. *Fox Broad. Co. v. Dish Network, L.L.C.*, 905 F. Supp. 2d 1088, 1111 (C.D. Cal. 2012)

First, with respect to the claims that DISH directly infringed Fox's copyrights in offering the PrimeTime Anytime service, the district court held, relying on the *Cablevision* decision, that because the subscriber is the one who decides whether to initiate the PrimeTime Anytime service, the subscriber not DISH is the one who makes the copies. The district court also held that notwithstanding the extent of DISH's control over which programs get recorded and the subscriber's inability to stop a recording in progress, DISH is not "the most significant and important cause" of the copying.

Second, with respect to the claims that DISH was secondarily liable under the Copyright Act for the conduct of its subscribers, the district court held that to establish derivative copyright infringement, direct infringement by a third party must be established. The district court held that DISH subscribers' conduct is no different than that of the consumers in the Supreme Court's decision in *Sony Corp. v. Universal City Studios, Inc.*, 464 U.S. 417 (1984) (the "*Betamax*" case), which involved copying programs to Betamax tapes with the ability to skip ads. Because the DISH subscribers would not be liable for direct copyright infringement, the district court held that DISH cannot be liable for secondary or derivative copyright infringement.

Fox immediately appealed the decision to the Ninth Circuit. Again, Fox lost. On July 24, 2013, the Ninth Circuit held that Fox did not demonstrate a likelihood of success on its copyright infringement claims regarding the PrimeTime Anytime and AutoHop services. *Fox Broad. Co. v. Dish Network L.L.C.*, 747 F.3d 1060 (9th Cir. 2014) (as amended). The Ninth Circuit, citing the *Cablevision* decision with approval, held that Fox failed to demonstrate a likelihood of success on its direct copyright infringement claim regarding PrimeTime Anytime, because infringement would require DISH to cause the copying, but here, because DISH's program creates the copy only in response to the subscriber's command, the subscriber causes the copying. The Ninth Circuit further held that Fox was unlikely to succeed on its claim of secondary copyright infringement

for the PrimeTime Anytime and AutoHop services. The court held that advertising skipping does not implicate Fox's copyright interest because Fox does not own the copyrights to the ads aired during commercial breaks. While Fox would later note that it in fact owns a copyright interest in ads promoting Fox programs, the district court would hold that the Ninth Circuit's holding on the merits of Fox's ad-skipping claims would have resulted in the same outcome.

## FOX EXPANDS LITIGATION SCOPE

### DISH Anywhere and Hopper Transfers

On February 21, 2013, during the appeal of the earlier preliminary injunction decision, Fox expanded the litigation by amending its complaint to include two additional DISH product offerings.

First, with respect to DISH's second-generation Hopper set-top box, loaded with Hopper, Sling and DISH Anywhere, which allows subscribers to view broadcast signals over the Internet, Fox claimed that DISH publicly performs Fox's copyrighted works by streaming them over the Internet and is secondarily liable for the conduct of its subscribers.

Second, with respect to a service called Hopper Transfers, which allows subscribers to copy programs saved on their Hopper DVRs to mobile devices, thereby enabling them to watch programs where they may not have Internet connectivity, Fox alleged that this service violated Fox's exclusive right to reproduce the works and made DISH secondarily liable for the conduct of its subscribers.

As it had with respect to PrimeTime Anytime and AutoHop, Fox moved for a preliminary injunction on the DISH Anywhere and Hopper Transfers products. On September 23, 2013, without reaching the question of whether Fox was likely to prevail on the merits of its claims, the district court again denied Fox's preliminary injunction motion. The district court held that "[i]f a plaintiff fails to establish that a significant threat of irreparable harm exists, the Court need not reach the likelihood that he would be successful on the merits of his claims." *Fox Broad. Co., Inc. v. Dish Network, L.C.C.*, No. CV 12-04529 DMG (SHx), 2013 U.S. Dist. LEXIS 187499 (C.D. Cal. Sept. 23, 2013).

As before, Fox immediately appealed to the Ninth Circuit. Fox lost again. On July 14, 2014, the Ninth Circuit, in a summary six-paragraph order, affirmed the district court's decision focusing on the failure to show irreparable harm without discussing the merits of Fox's claims. *Fox Broad. Co. v. Dish Network L.L.C.*, No. 13-56818, 2014 U.S. App. LEXIS 13348 (9th Cir. July 14, 2014).

## DISH ALSO PREVAILS IN THE EARLY ROUNDS IN NY

Separately, on November 23, 2012, in its case pending in the Southern District of New York, ABC also moved for a preliminary injunction against DISH based on the PrimeTime Anytime and AutoHop features. ABC's preliminary injunction motion met the same fate as Fox's motion.

On September 18, 2013, the district court denied ABC's motion for a preliminary injunction. *DISH Network, L.L.C. v. ABC, Inc. (In re AutoHop Litig.)*, No. 12 Civ. 4155 (LTS) (KNF), 2013 U.S. Dist. LEXIS 143492 (S.D.N.Y. Sept. 18, 2013). With respect to ABC's direct infringement claim, the district court found that ABC had failed to demonstrate "likelihood of success on its direct copying cause of action because the evidentiary record indicates, and the Court finds, that the consumer makes the copy [such that there] is thus no factual basis upon which DISH could be found liable for direct infringement of ABC's right of reproduction." With respect to the secondary infringement claim, the district court found that DISH had "demonstrated that it is likely to succeed in carrying its burden of demonstrating that its subscribers' time-shifting constitutes fair use [and that] ABC has failed to demonstrate that it is likely to succeed on the merits of its claim of secondary or vicarious infringement."

> ***Aereo*** **should be limited to companies that engage in conduct like Aereo.**

ABC appealed the decision. While the Second Circuit heard oral argument on February 20, 2014, the court never got the opportunity to decide the appeal.

## ABC AND CBS SETTLE WITH DISH

On March 3, 2014, ABC and DISH issued a press release announcing that the parties had reached a settlement of the dispute in connection with the renewal of the carriage agreement. Of critical importance to DISH, the agreement granted DISH the "rights to stream cleared linear and video-on-demand content from the ABC-owned broadcast stations, ABC Family, Disney Channel, ESPN and ESPN2, as part of an Internet delivered, IP-based multichannel offering." Thus, the renewal agreement set the groundwork for DISH to be able to launch its Sling TV, which is a first-of-its-kind, over-the-top offering that includes ESPN sports programming. Of critical importance to ABC, DISH agreed to "disable AutoHop functionality for ABC content within the C3 ratings window." Thus, DISH subscribers would now have to wait until three days had passed before

they could play back primetime ABC programming while automatically skipping the advertisements.

Similarly, on December 6, 2014, CBS and DISH issued a press release announcing a renewal of their carriage agreement and the settlement of the litigation. The parties announced that "[t]he agreement will result in dismissal of all pending litigation between the two companies, including disputes over PrimeTime Anytime and AutoHop [and that as] part of the accord, DISH's AutoHop commercial-skipping functionality will not be available for CBS Television Network-owned stations and affiliates during the C7 window." Thus, DISH subscribers would now have to wait until seven days had passed before they could play back primetime CBS programming while automatically skipping the advertisements.

## THE FOX SUMMARY JUDGMENT DECISION

On August 22, 2014, in the California action, Fox and DISH filed opposing motions for summary judgment on Fox's copyright claims with respect to the AutoHop, PrimeTime Anytime, DISH Anywhere, and Hopper Transfers product offerings.

On October 17, 2014, the district court, from the bench promising a written decision to follow, provided the parties with its tentative decision on the claims. With respect to each of the core product offerings, the district court noted that it was inclined to rule in favor of DISH.

On January 12, 2015, the district court issued its written summary judgment decision under seal. Shortly thereafter, DISH and Fox filed a joint stipulation noting that the current Fox carriage agreement expires on October 29, 2015, that "DISH has settled similar disputes with both ABC and CBS in the context of renewals of their respective … agreements," and that the parties "believe it highly likely that the negotiation later this year of a renewal of their 2010 agreement will result in resolution of this lawsuit." The parties proposed keeping the summary judgment order under seal during the stay, claiming that "unsealing the Order may impair the parties' ability to reach a resolution of the case."

Although it granted the stay motion, the district court denied Fox's and DISH's request to keep the summary judgment order under wraps. On January 21, 2015, the district court unsealed its written summary judgment decision, which revealed a clean sweep for DISH on Fox's copyright claims regarding the core product offerings, AutoHop, PrimeTime Anytime, DISH Anywhere and Hopper Transfers.

In reaching the decision, the district court rejected the expansive reading of the Supreme Court's decision in *ABC, Inc. v. Aereo, Inc.*, 134 S. Ct. 2498 (2014) that Fox advocated. While Fox argued the *Aereo* decision was a "game-changer," the district court disagreed, noting the Supreme Court's "effort to cabin the potential overreach of its decision" and its express admonition that "its 'limited holding' should not be construed to 'discourage or to control the emergence of use of different kinds of technologies.'" The district court found that *Aereo* should be limited to companies that engage in conduct like Aereo, stating that "Aereo's holding that entities bearing an 'overwhelming likeness' to cable companies publicly perform within the meaning of the Transmit Clause does not extend" to DISH's product offerings.

Contrary to Fox's suggestion, the district court further expressly held that the volitional conduct doctrine survives the *Aereo* case. The district court held "[t]he volitional conduct doctrine is a significant and long-standing rule, adopted by all Courts of Appeal to have considered it, and it would be folly to presume that *Aereo* categorically jettisoned it by implication."

## WHAT LIES AHEAD

With CBS and ABC having already settled with DISH and a settlement with Fox likely to be completed before the expiration of the parties' current carriage agreement in October 2015, NBC would then be left as the last remaining network with which DISH has not reached an accord.

In comparison to these other networks, NBC has not been active in the litigation. Pursuant to an August 6, 2014 stipulation between the parties, the NBC action was stayed until a final judgment in the Fox action. To date, no action has been taken to lift the stay. In light of the March 2013 acquisition of NBC by Comcast, it is questionable whether NBC has the same interest in pressing copyright claims that, if successful, could limit the rights of a programming distributor like Comcast. Thus, one would imagine that DISH and NBC will likely also reach an accord.

If the recent summary judgment decision in the Fox action marks the end of the road for the litigation, these rulings with respect to ad-skipping, the automated wholesale copying of programming blocks and place-shifting devices such as DISH Anywhere and Hopper Transfers, will likely provide greater license for distributors to offer these products to their subscribers and limit the copyright owners' ability to prevent the distribution of their works through new distribution channels.

*This article originally appeared in the Intellectual Property Strategist.*

# THE NEW FRONTIER IN INTEREST-BASED ADVERTISING: FTC SHIFTS FOCUS TO CROSS-DEVICE TRACKING

**By Julie O'Neill and Patrick Bernhardt**

As consumers increasingly connect to the Internet using multiple devices—such as mobile phones, tablets, computers, TVs and wearable devices—advertising technology companies have rapidly developed capabilities to reach the same consumers across their various devices. Such "cross-device" tracking enables companies to target ads to the same consumer regardless of the platform, device or application being used. Recently, the Federal Trade Commission (FTC) announced that it will host a workshop on November 16, 2015, to explore the privacy issues arising from such practices—signaling that interest-based advertising (IBA) is still at the forefront of its agenda.

For a long time, advertisers and publishers have tracked consumers' online activities using HTTP cookies stored in web browsers on desktop and laptop computers. In response to the FTC's concerns over consumers' visibility into and control over such tracking for IBA purposes, industry responded with widely-adopted ways for publishers and advertisers to provide consumers with enhanced notice and cookie-based choice with respect to such tracking.

As consumers' behavior has shifted, however, traditional cookie-based technologies are becoming less effective. Most consumers now access the Internet through apps on various platforms, in addition to web browsers, and they tend to use different devices throughout the day. This presents challenges for advertisers, publishers and others who want a complete picture of how individual consumers interact with their websites, services and advertisements over time—as well as for those who want to know where and how they can reach such consumers. In response, companies have developed various solutions for identifying the same consumer across devices. One approach, for example, is to use "deterministic" methods that link the consumer's devices to a single account as the consumer logs into websites and services on different devices. Another is through "probabilistic" methods that infer links among devices that share similar attributes, such as location derived from IP address. In some cases, companies may combine multiple techniques for greater accuracy.

**The FTC is focused on ever more sophisticated ways to track consumers in order to deliver interest-based ads to them.**

In its announcement, the FTC explained that these new practices may raise privacy issues if consumers are not provided with adequate notice and control—and the workshop will address, among other topics, how companies can make their tracking more transparent and give consumers greater control over it. If history is a guide, the FTC will likely publish a staff report some months after the workshop, to highlight the privacy issues it sees with cross-device tracking and to offer industry guidance on addressing them.

The FTC's announcement is a natural extension of its recent workshops on mobile privacy disclosures, the Internet of Things and mobile device tracking. It also follows recent news from the Digital Advertising Alliance (DAA) that it has launched tools to provide in-app notice and choice to consumers about IBA practices and that it expects enforcement of the DAA Self-Regulatory Principles in the mobile environment to begin this summer.