Volume 8, Issue 2, April 2017

SOCIALLY AWARE

THE SOCIAL MEDIA LAW UPDATE

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

IN THIS ISSUE

EDITORS

John F. Delaney
Aaron P. Rubin

CONTRIBUTORS

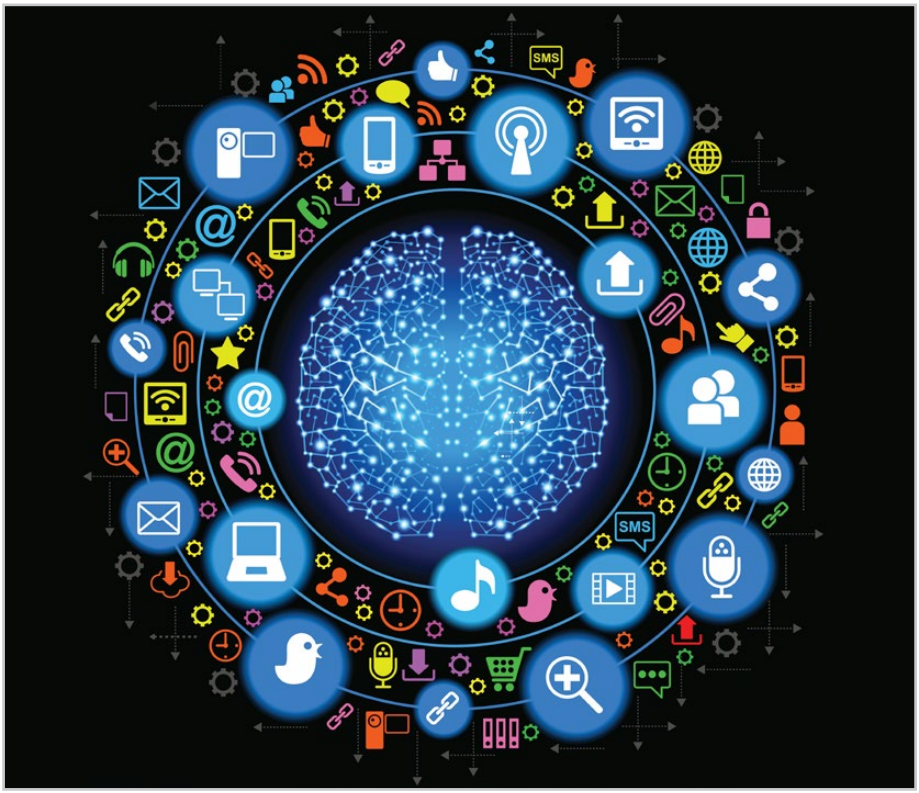
John P. Carlin
Abigail L. Colella
John F. Delaney
Mona Fang
Adam J. Fleisher
J. Alexander Lawrence
Julie O'Neill
Joseph Roth Rosner
Aaron P. Rubin
Ronan Tigner
Alex van der Wolk

FOLLOW US

Morrison & Foerster's Socially Aware Blog

@MoFoSocMedia

MORRISON FOERSTER

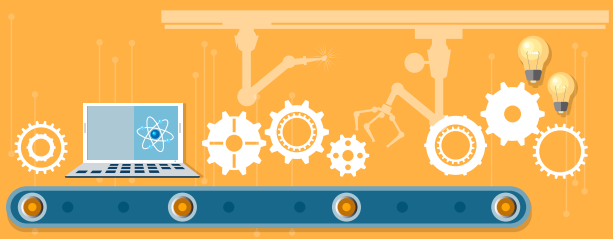


Welcome to the newest edition of *Socially Aware*, our Burton Award-winning guide to the law and business of social media.

In this edition, we explore the threat to U.S. jobs posed by rapid advances in emerging technologies; we examine a Federal Trade Commission report on how companies engaging in cross-device tracking can stay on the right side of the law; we take a look at a Second Circuit opinion that fleshes out the "repeat infringer" requirement online service providers must fulfill to qualify for the Digital Millennium Copyright Act's safe harbors; we discuss a state court decision holding that Section 230 of the Communications Decency Act immunizes Snapchat from liability for a car wreck that was allegedly caused by the app's "speed filter" feature; we describe a recent decision by the District Court of the Hague confirming that an app provider could be subject to the privacy laws of a country in the European Union merely by making its app available on mobile phones in that country; and we review a federal district court order requiring Google to comply with search warrants for foreign stored user data.

All this—plus an infographic illustrating how emerging technology will threaten U.S. jobs.

THE LOSS OF JOBS TO AUTOMATION



As many as **47% of U.S. jobs** could be automated in the next 20 years.[1]

85% **85% of U.S. manufacturing job losses** from 2000 to 2010 were due to automation and other technological change.[2]

5M By 2020, technological advances could result in the loss of more than **five million jobs in the world's leading economies**.[3]

65% Approximately **65% of children starting school now** will wind up in occupations that don't exist today.[4]

39% of people who work in the legal field could lose their jobs in the next decade[5]

1.7 million U.S. truckers also risk losing their jobs in the next 10 years[6]

30% of banking jobs (such as financial analysts) could be eliminated between 2015 and 2025[7]

People who earn $20 per hour or less have an **83%** chance of losing their jobs in the next five years[8]

SOURCES

1. https://www.linkedin.com/pulse/5-jobs-robots-take-first-shelly-palmer
2. https://www.ft.com/content/dec677c0-b7e6-11e6-ba85-95d1533d9a62
3. http://money.cnn.com/2016/01/18/news/economy/job-losses-technology-five-million/
4. http://money.cnn.com/2016/01/18/news/economy/job-losses-technology-five-million/
5. http://www.refinery29.com/2017/01/136970/jobs-most-likely-to-be-automated-robots
6. http://www.ttnews.com/articles/basetemplate.aspx?storyid=43407&page=3
7. http://money.cnn.com/2016/04/04/investing/bank-jobs-dying-automation-citigroup/
8. https://www.linkedin.com/pulse/5-jobs-robots-take-first-shelly-palmer

TECH, NOT TRADE, POSES BIGGEST THREAT TO AMERICAN JOBS

By John F. Delaney

Donald Trump's successful road to the White House was fueled by heated rhetoric against free trade deals and U.S. companies engaged in offshore outsourcing. Underpinning his slogan "Make America Great Again" was a premise that millions of jobs lost to other countries should and could return to the United States.

The president's ambitious goals include the creation of 25 million new jobs over 10 years. Central to the plan is adjusting trade policies—either scrapping them altogether or negotiating new ones more beneficial to American workers. So, too, it would seem, are policies aimed at discouraging companies from outsourcing operations abroad where labor is cheaper.

During the campaign, President Trump called out some of America's best-known companies for their reliance on foreign labor. He has kept up the rhetoric since being elected. In December, when he touted his success in persuading air conditioner maker Carrier Corp. to keep 800 jobs in Indiana, Trump signaled a policy of retribution to prevent further outsourcing: "Companies are not going to leave the United States any more without consequences," he said.

Some economists view President Trump's plans with skepticism. They note, for instance, that trade deals generally have little overall impact on jobs. Additionally, his threats to companies engaged in outsourcing would face practical obstacles. Levying punitive taxes on individual companies, for example, would probably require Congressional approval. Even if such a policy were put into place, it would not likely improve American competitiveness. After all, the U.S. cannot prevent non-U.S. companies from using low-cost labor to make less expensive goods.

The bigger problem is that President Trump's focus on trade and outsourcing appears to be misplaced. The real long-term threat to American jobs isn't foreign labor; it's the accelerating pace of technological disruption eliminating jobs altogether.

We're on the cusp of seeing entire job categories disappear—not move offshore, but vanish—because of rapid advances in artificial intelligence, robotics, automation, cloud computing and other emerging technologies. A World Economic Forum survey of executives at large companies estimated that five million jobs in the world's leading economies could disappear over the next five years. And a just-released study by PwC found that robots and automation could result in the loss of almost 40% of U.S. jobs over the next 15 years.

It doesn't require a vivid imagination to foresee some of the potential destruction.

As just one example, consider the four million Americans who make their living behind the wheel. With rapid advances in self-driving vehicle technology, their future is under a dark cloud. Some suggest the 1.7 million truck drivers are especially vulnerable, given that they spend most of their time on the highway where human intervention is needed least. Then there is the tremendous financial incentive: In the $700 billion trucking industry, an estimated third of costs go to compensating drivers. The temptation among trucking companies to cut those costs—and gain a competitive advantage—will be great.

> The real long-term threat to American jobs isn't foreign labor; it's the accelerating pace of technological disruption eliminating jobs altogether.

Similarly, the potential widespread adoption of block chain technology could lay waste to millions of jobs in the financial services industry. The technology is now used to record and store Bitcoin payments, but startups and large banks are exploring ways to use it to improve a variety of other services and compliance tasks, which could save billions.

Automating tasks—a core function of many of these new technologies—is nothing new. But the pace of automation's march into areas beyond the assembly line is hard to overstate. Consider the now ubiquitous ATM or the airport kiosk. The march won't stop. A new restaurant with a machine capable of making a gourmet hamburger in 10 seconds, for example, is set to open in San Francisco. In Japan, an insurance company laid off workers following the company's adoption of IBM's Watson Explorer, an artificial intelligence system that will perform an important back office function at the company.

Of course, not all automating technologies will lead to the elimination of jobs. But if the White House is committed to massive and sustained job growth, it will need to confront the inevitable, relentless advance of disruptive new technologies.

Andrew McAfee and Erik Brynjolfsson of the MIT Initiative on the Digital Economy have blamed new technologies on the "great decoupling" of productivity and job growth rates. After World War II, the two rates rose in near lockstep for decades, but beginning in 2000 job growth slowed considerably compared to productivity. President Trump's promise to reduce bureaucracy and roll back regulation may well fuel the growth of these new technologies, leading to more rapid displacement of workers than might have otherwise occurred.

History has shown that new technologies create new jobs even as they kill off old ones. After talkie movies were introduced in the late 1920, for example, movie theatres no longer needed piano players to provide accompaniment to movies. But new job opportunities opened in Hollywood for audio engineers. The more recent innovation of online banking has surely limited the need for traditional bank tellers, but it has created new jobs for programmers.

So yes, technology creates jobs, but mostly for the skilled worker capable of exploiting the new opportunities. The truck driver, and other low-skilled workers facing disruptive technologies that threaten their livelihood, are in a much more precarious position. For many truck drivers, becoming a software programmer for self-driving vehicles or a drone-repair person isn't possible absent extensive training.

Moreover, the pace of technology-driven disruption is accelerating as new technologies combine and mutate in often unexpected ways. Autonomous vehicles using block chain technology for payment transactions will mean job losses for taxi drivers *and* bank employees. Commercial drones combined with big data analytics relying on cloud storage will mean less need for delivery personnel *and* supply chain managers.

Along with most elected officials, President Trump has been silent on this key issue. He ignores it at his own political peril. To make good on his campaign promises, his administration will want to focus on training displaced workers for these new emerging jobs, many of which will require programming, engineering or similar skills.

President Trump clearly knows a thing or two about disruption—his upset victory last November is proof of that. But will he be able to get out ahead of the coming wave of low-skilled job losses arising from disruptive technologies? Doing so would help him address what threatens to be a growing source of economic anxiety among American workers.

A version of this article originally appeared in *MarketWatch*

FTC REPORT REINFORCES THE RULES FOR CROSS-DEVICE TRACKING

By Julie O'Neill, Adam J. Fleisher and Joseph Roth Rosner

Well over a year after holding a workshop addressing privacy issues associated with cross-device tracking, Federal Trade Commission (FTC) staff have issued a report. The report sets the stage by describing how cross-device

tracking works, noting its "benefits and challenges," and reviewing (and largely commending) current industry self-regulatory efforts.

The report also makes recommendations, which—while building upon the staff's traditional themes of transparency and choice—do not introduce any materially new suggestions for compliance.

The staff's recommendations do not have the force of law, but they do indicate the steps that the staff believes a company should take in order to avoid a charge of unfairness or deception under Section 5 of the FTC Act.

A QUICK REVIEW OF CROSS-DEVICE TRACKING

As more consumers utilize multiple devices in their daily lives, more and more companies are using new technologies to attempt to ascertain that multiple devices are connected to the same person. This is generally done through the use of either deterministic information (e.g., by recognizing a user through the log-in credentials he or she uses across different devices) or probabilistic information (i.e., by inferring that multiple devices are used by the same person based on information about the devices, such as IP address, location and activities on the devices).

As the FTC staff note in the report, cross-device tracking provides many benefits. For instance, it enables a seamless experience for users across their devices and can also help improve fraud detection by identifying devices *not* previously associated with a known user.

Moreover, cross-device tracking facilitates a better online advertising experience by, among other things, more effectively targeting advertisements to users. The practice also, however, raises privacy concerns because it may not be adequately disclosed to consumers, and consumers may not be able to readily control it.

STATE OF PLAY

In response to earlier FTC statements on the privacy issues raised by cross-device tracking, industry expanded the existing interest-based advertising (IBA) self-regulatory regime to specifically address cross-device tracking. Enforcement of the Digital Advertising Alliance (DAA) cross-device tracking principles began on February 1, 2017.

> The FTC report does not suggest changes to the notice and choice required by the DAA principles for cross-device tracking. There had been some speculation that FTC staff might recommend consumers be given a way to universally opt out across all of their linked devices.

These principles apply the DAA's IBA self-regulatory notice-and-choice regime to cross-device tracking if browsing activity on one device is used to deliver ads on another device. In such scenarios, the DAA principles require that consumers be provided with a device-specific opt-out from both (1) the collection of data on the specific device in order to deliver IBA on *other* devices; and (2) the delivery of IBA on that device based on information collected from another device.

THE STAFF REPORT—STATUS QUO PRESERVED?

While the FTC staff report commends the IBA self-regulatory efforts of both the DAA and the Network Advertising Initiative, it also suggests that they could "strengthen their efforts." Importantly, however, the report does not suggest changes to the notice and choice required by the DAA principles at this time. There had been some speculation that the staff might recommend that consumers be given a single way to opt out across all of their linked devices. It did not. Instead, staff acknowledged that current technological limitations would make it difficult to offer such a universal opt-out. The staff did suggest that companies "continue to reassess technical limitations and simplify consumer choices whenever possible."

While not upsetting the current self-regulatory approach, the report, nonetheless, provides suggestions about how basic privacy principles can be adapted to cross-device tracking:

Transparency. The report recommends increased transparency and truthfulness, including about the types of data collected and how it is used and shared. Reinforcing statements by former FTC Chairwoman Edith Ramirez (*see* here), the report states that personally identifiable information includes any information that can be *reasonably linked* to a consumer or *a consumer's device*. The staff accordingly suggests that "companies that provide raw or hashed email addresses or usernames to cross-device tracking companies should refrain from referring to this data as anonymous or aggregate, and should be careful about making blanket statements to consumers stating that they do not share 'personal information' with third parties."

Choice. Any opt-out that a company offers must be clear and effective. Moreover, its scope must be accurate and not misleading. For example, if an opt-out is effective only with respect to the device from which it is exercised, that fact should be clear from the opt-out instructions, and consumers should not be led to believe that the opt-out extends to all of their devices.

Opt-In for Sensitive Data. Consistent with the FTC's overall approach to sensitive data, the report recommends that companies obtain express consent to collect four types of sensitive information: health, financial, precise geolocation and children's information. Companies are encouraged to take a broad approach in this regard, given the ease with which sensitive information may be pieced together from activity across devices. For example, the use of a diabetes-related mobile app or a visit to an AIDS education website could be tantamount to the collection of sensitive information.

Security. The report recommends that companies have reasonable security measures in place to avoid unauthorized access to and use of the personal information within their control. As part of this, and consistent with the FTC's standard refrains regarding data minimization and deletion, the report recommends that companies keep only the information that is necessary for their business purposes.

Cross-device tracking is becoming more prevalent, and the FTC is paying attention. Companies involved in tracking and targeting users across devices should consider the report's recommendations when designing or revisiting their compliance strategies.

SECOND CIRCUIT CLARIFIES "REPEAT INFRINGER" POLICY REQUIREMENT FOR DMCA COPYRIGHT SAFE HARBORS

By J. Alexander Lawrence and Abigail L. Colella

Congress enacted the Digital Millennium Copyright Act (DMCA) nearly two decades ago seeking to balance the needs of two factions: content creators, who were struggling to protect their intellectual property in the digital age, and fledgling Internet companies, who feared being held liable for the misdeeds of their customers.

For the Internet companies, Congress offered relief by creating a number of "safe harbors" shielding such companies from copyright-related damages arising from their customers' infringing activities.

In particular, the DMCA established four distinct safe harbors for online service providers, each safe harbor aimed at a different type of online activity (i.e., transitory digital network communications; system caching; online hosting; and provision of information location tools) and each with its own set of eligibility requirements.

To qualify for *any* of these DMCA safe harbors, however, the DMCA requires that service providers "reasonably implement" a policy that provides for the termination of "repeat infringers" in "appropriate circumstances."

Despite the threshold importance of repeat infringer policies, the DMCA left many questions unanswered. Who exactly counts as an "infringer"? Does it include every user accused of infringement or only those found culpable in court? If it's somewhere in between, what level of proof is required before a service provider is required to take action? Can the repeat infringer policy differentiate between those who upload infringing content for others to copy and share and those who only download such content for their own personal viewing? And how many acts of infringement does it take to become a "repeat infringer" anyway?

When the Second Circuit Court of Appeals recently denied rehearing en banc and issued a modified opinion in *EMI v. MP3tunes*, it added its voice in the limited—but growing—number of cases addressing these questions. The *MP3tunes* case involves two websites founded in 2005 by Internet entrepreneur Michael Robertson. (Mr. Robertson is also the founder and CEO of MP3.com, which, only a few years earlier, had been held liable for widespread copyright infringement.)

The first of Mr. Robertson's two websites at issue, mp3tunes.com, was an early cloud storage "locker" for digital music. The second website, sideload.com, allowed users to search the Internet for "free" music files and then copy (i.e. sideload) those files directly to their online locker. Many of these files allegedly contained pirated music, and, in 2007, EMI sued MP3tunes and Mr. Robertson for copyright infringement.

> Reevaluating the meaning of "repeat infringer," the Second Circuit noted that infringement is a strict liability offense with no requirement to prove unlawful intent. Moreover, both uploading and downloading can constitute infringement.

In a 2011 summary judgment decision, Judge Pauley, a federal judge in Manhattan, held that, as a matter of law, MP3tunes had reasonably implemented a repeat infringer policy under the DMCA; in support of his decision, Judge Pauley noted that the company had instituted a policy for responding to DMCA takedown requests and had actually "terminated the accounts of 153 users who allowed others to access their

lockers and copy music files without authorization." The court's analysis, however, used a narrow definition of "repeat infringers," including only those who *upload* infringing content to the Internet with *knowledge* that the content is infringing. The court explained:

MP3tunes' users do not upload content to the internet, but copy songs from third-party sites for their personal entertainment. There is a difference between (1) users who know they lack authorization and nevertheless upload content to the internet for the world to experience or copy, and (2) users who download content for their personal use and are otherwise oblivious to the copyrights of others.

Despite the court's validation of the MP3tunes repeat infringer policy, the jury ultimately found the company willfully blind to infringing activity by its customers and thus ineligible for DMCA safe harbor protection.

On appeal, a panel of judges on the Second Circuit found that the district court had erred, both regarding the definition of "repeat infringer" and on whether MP3tunes's repeat infringer policy was reasonable as a matter of law.

Reevaluating the meaning of "repeat infringer," the Second Circuit noted that infringement is a strict liability offense with no requirement to prove unlawful intent. Moreover, both uploading *and downloading* can constitute infringement. Because the DMCA does not define "repeat infringer," the court adopted this ordinary meaning and held that "all it [takes] to be a 'repeat infringer' [is] to repeatedly [upload or download] copyrighted material for personal use."

Next, the Second Circuit found that MP3tunes's repeat infringer policy was not, in fact, reasonable as a matter of law because, while the site did respond to takedown notices from copyright owners and terminated the accounts of some users, "MP3tunes did not even try to connect known infringing activity of which it became aware through takedown notices to users who repeatedly sideloaded files and created links to that infringing content in the sideload.com index."

Requiring this sort of search would seemingly run up against a separate DMCA provision that prohibits the conditioning of safe harbor protection on "a service provider monitoring its service or affirmatively seeking facts indicating infringing activity." The Second Circuit, however, found that such a search would *not* constitute "monitoring" or "affirmatively seeking facts" under the DMCA because "MP3tunes would simply have had to make use of information already within its possession"—the takedown notices provided by EMI—"and connect that information to known users."

In the wake of the decision, several high-powered *amici*, including Dropbox, Facebook, Google, Pinterest and Twitter, took issue with the Second Circuit's approach to repeat infringer policies and joined in supporting MP3tunes's petition for rehearing before the full Second Circuit. Specifically, these leading Internet companies were concerned that requiring service providers to "tally strikes and terminate users merely for having accessed, viewed, or otherwise engaged with content that later might be the subject of a takedown notice" would destabilize the DMCA safe harbor regime and unfairly penalize users. The Second Circuit was unmoved and denied rehearing by the full court. MP3tunes has since indicated that it will seek Supreme Court review of Robertson's personal jurisdiction issues, but the Second Circuit has had the final say on the copyright question.

Also on the horizon is a similar dispute that may provide further guidance in this area. Later this year, the Fourth Circuit Court of Appeals is slated to review a lower court decision in *BMG v. Cox*, which turns on whether "repeat infringers" includes all users accused of infringement or only cases of infringement adjudicated in courts. The district court squarely rejected Cox's "adjudicated infringer" position late last year, and *MP3tunes* does little to signal sympathy for that reading, but, in an area with little case law, the issue is far from settled.

In the meanwhile, companies that host or otherwise engage with user-generated content will want to revisit their current repeat infringer policies and determine whether such policies should be updated in light of emerging DMCA safe harbor case law.

SNAPCHAT CLOCKS SECTION 230 WIN IN SPEED FILTER CASE

By Aaron P. Rubin and Mona Fang

We have been monitoring a trend of cases narrowing the immunity provided to website operators under Section 230 of the Communications Decency Act (CDA). A recent decision by a state court in Georgia, however, demonstrates that Section 230 continues to be applied expansively in at least some cases.

The case, *Maynard v. McGee*, arose from an automobile collision in Clayton County, Georgia. Christal McGee, the defendant, had allegedly been using Snapchat's "speed filter" feature, which tracks a car's speed in real-time and superimposes the speed on a mobile phone's camera view. According to the plaintiffs, one of whom had been injured in the collision, McGee was using the speed filter when the accident occurred, with the intention of posting a video on Snapchat showing how fast she was driving. The plaintiffs sued McGee and Snapchat for negligence, and Snapchat moved to dismiss based on the immunity provided by Section 230.

The plaintiffs alleged that Snapchat was negligent because it knew its users would use the speed filter "in a manner that might distract them from obeying traffic or safety laws" and that "users might put themselves or others in harm's way in

order to capture a Snap." To demonstrate that Snapchat had knowledge, the plaintiffs pointed to a previous automobile collision that also involved the use of Snapchat's speed filter. The plaintiffs claimed that "[d]espite Snapchat's actual knowledge of the danger from using its product's speed filter while driving at excessive speeds, Snapchat did not remove or restrict access to the speed filter."

Section 230(c) of the CDA provides that "no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." The plaintiffs argued that the Section 230 immunity did not apply to Snapchat in this case, however, because Snapchat's negligence was based on its own content—i.e., the speed filter—rather than on content posted by McGee (note that McGee did not actually post a video to Snapchat before the collision occurred). Specifically, the plaintiffs asserted that Snapchat should have removed the speed filter after it learned of the previous accidents that the feature allegedly caused.

The court was not persuaded, however, and noted that "decisions about the structure and operation of a website—such as decisions about features that are part and parcel of the site's overall design—reflect choices about what content can appear on the website and in what form and thus fall within the purview of traditional publisher functions" (internal quotation marks omitted).

The court also found that Snapchat's knowledge of prior accidents allegedly caused by the speed filter was knowledge that Snapchat "would have obtained because it created the 'speed filter' and was aware of what was published on its application," which further convinced the court that plaintiffs were seeking to impose a duty in Snapchat that "derives from Snapchat's status or conduct as a publisher." Finally, the court determined that a user's choice to use the speed filter "is not Snapchat's speech, but is ultimately the user's speech using the voluntary options [of] Snapchat's platform."

The court saw plaintiffs' injuries as flowing from McGee's choice to use the speed filter and determined that Section 230 precluded plaintiffs from holding Snapchat liable for her decision.

For these reasons, the court held that the plaintiffs were seeking to hold Snapchat liable as a publisher and that such liability was precluded by Section 230. Accordingly, the court dismissed the plaintiffs' claims. But it's worth noting that, while the court acknowledges that Section 230 applies only to third-party content and does not immunize a publisher's own content, the actual analysis in the decision seems to treat any "publisher" activity as automatically immunized without regard to the source of the content at issue.

For example, while it is certainly true, as the court notes, that "decisions relating to the monitoring, screening, and deletion of content" are traditionally publisher activities, that fact is relevant to Section 230 only when the content at issue is provided by a user or other third party. If the publisher is making choices about its own content—as plaintiffs alleged was the case with Snapchat and its decision to continue providing the speed filter with knowledge that it had caused accidents in the past—then the mere fact that content-related decisions are traditional publisher activities does not necessarily mean that Section 230 applies.

In any event, while the court's analysis may raise a few questions, the result is generally in line with prior cases applying Section 230 immunity to offline injuries caused by third-party defendants, as other commentators have noted. Ultimately, it seems that the court saw plaintiffs' injuries as flowing from McGee's choice to use the speed filter and determined that Section 230 precluded plaintiffs from holding Snapchat liable for her decision to use a feature that Snapchat, in its role as a publisher, made available. For fans of Section 230, *Maynard v. McGee* is a welcome indication that the statute's "robust immunity" lives on, at least sometimes.

THE HAGUE DISTRICT COURT'S WHATSAPP DECISION CREATES CONCERNS FOR MOBILE APP DEVELOPERS

By Alex van der Wolk and Ronan Tigner

Can the mere offering of a mobile app subject the provider of such app to the privacy laws of countries in the European Union (EU)—even if the provider does not have any establishments or presence in the EU? The answer from the District Court of The Hague to that question is yes. The court confirmed on November 22, 2016, that app providers are subject to the Dutch Privacy Act *by virtue of the mere offering of an app that is available on phones of users in the Netherland, even if they don't have an establishment or employees there.*

Context. EU privacy laws generally apply on the basis of two triggers: (i) if a company has a physical presence in the EU (in the form of an establishment or office or otherwise) and that physical presence is involved in the collection or other handling of personal information;

or (ii) if a company doesn't have a physical presence but makes use of equipment and means located in the EU to handle personal information.

Background. In 2013, the Dutch Data Protection Authority (DPA) completed an investigation into WhatsApp's practice of asking users, including in the Netherlands, to give access to their electronic address book to WhatsApp and enable it to record phone numbers, including those of non-WhatsApp users on its U.S. servers. Further to the investigation, the DPA ordered that the company appoint a representative in the Netherlands accountable for compliance with the Dutch Privacy Act under Article 4 of the Act (i.e., where a company who processes personal information of users does not have an establishment in the Netherlands but uses equipment there).

> Simply by making an app available in the Netherlands, the company made 'use of equipment.'

Key findings. The court decided that, simply by making an app available in the Netherlands, the company made "use of equipment" (i.e., smartphones on which the app is installed) in the Netherlands, even though the equipment is not the company's own or specifically procured equipment. The court also found that such equipment was used for processing personal information (e.g., accessing users' address books and transferring certain information to the United States). As a result, this triggered the application of EU privacy rules, as implemented in the Netherlands, through the Dutch Privacy Act.

The court also refuted the company's argument that a representative must only be appointed in the EU in the context of information and reporting duties to the DPA and not substantive compliance with the Dutch Privacy Act. To the contrary, the court found that this representative had to comply with the full breadth of the Dutch Privacy Act.

To support its view, the court referred to works (on applicable law and apps on smart devices) of the Article 29 Working Party (WP29, a consortium of EU Member State DPAs) and to the European Court of Justice's interpretation of the scope of EU privacy rules in the *Google v. Spain* case (i.e., Google's search engine is subject to EU privacy rules even though the search engine is administered out of the U.S., C-131/12).

It is interesting to note that the court relies on the WP29 in reaching its decision. Although the court refers to the WP29's work as "advice," thereby acknowledging that it is not binding, the court nevertheless cites to such advice in support of its own findings and ruling.

Conclusion. App developers will want to take note of the District Court of The Hague's *WhatsApp* decision, given that it appears to significantly broaden the reach of EU privacy rules.

Apps are almost always provided on a global basis. Under the *WhatsApp* decision, the mere fact that an app developer has customers in the EU, and has access (even at a distance) to such user's personal information, may mean that it needs to comply with EU privacy rules, including appointing a representative in the EU. An app developer seeking to avoid this obligation may need to either geo-restrict the availability of its app (e.g., restrictions in app stores) or refrain from collecting users' information (e.g., this could work for purely informative apps).

Finally, although this "use of equipment" criteria will disappear under the new EU privacy regime (the General Data Protection Regulation, effective as of May 25, 2018), it will be replaced by new criteria for applicability, including the offering of products or services to EU residents. It may well be likely (although this was not before the court in the *WhatsApp* case) that a court will reach a similar conclusion also under that new EU privacy regime.

The District Court of The Hague's decision is available here.

GOOGLE ORDERED TO COMPLY WITH WARRANT FOR FOREIGN-STORED USER DATA

By John P. Carlin and Joseph Roth Rosner

In a major development for cloud and other data storage providers, and further complicating the legal landscape for the cross-border handling of data, a Federal Magistrate Judge in the Eastern District of Pennsylvania ruled for the Department of Justice and ordered Google, Inc., to comply with two search warrants for foreign-stored user data. The order was issued on February 3, 2017 pursuant to the Stored Communications Act, (SCA), and the reasoning of the Court rested heavily on the court's statutory analysis of the SCA. The ruling is a marked departure from a recent, high-profile Second Circuit decision holding that Microsoft could refuse to comply with a similar court order for user data stored overseas.

The SCA regulates how service providers like Google and Microsoft who store user data can disclose user information. The Magistrate Judge issued two warrants under the SCA for emails sent from Google users in the United States to recipients in the United States. Google refused to fully comply, invoking *Microsoft*, and the Government moved to compel. In its briefing, Google argued that the SCA can only reach data stored in the United States and that, because Google constantly shuffles "shards" of incomplete user data between its servers

across the world, Google could never know for certain what information is stored domestically and what is stored overseas. Therefore, Google argued, the data sought under the warrants was beyond the reach of the SCA.

> The key inquiry, the Court reasoned, is where the 'relevant conduct' affecting privacy takes place.

The Court ordered Google to comply with the warrants. Citing *Microsoft*, the Court began by noting that the focus of the SCA was to preserve the privacy of individuals' communications, and that the SCA—and any warrant issued pursuant to it—applies only within the United States. The key inquiry, the Court reasoned, is *where* the "relevant conduct" affecting privacy takes place. On this, the Court "respectfully disagree[d]" with the Second Circuit's reasoning. In *Microsoft*, the seizure of data in Ireland was deemed the relevant conduct. But as for Google, the Court found, the relevant conduct was "the actual invasion of the account holders' privacy—the searches—[that] will occur in the United States." Transferring the data to the U.S. would not constitute an illegal seizure under the Fourth Amendment, the Court reasoned, because "there is no meaningful interference with the account holder's possessory interest in the user data." That leaves only "a permissible domestic application of the SCA, even if other conduct (the electronic transfer of data) occurs abroad."

The Court was critical of two aspects of Google's position in particular. First, if the certain location of user information was never known, then Google could not specify *which* foreign sovereignty would be violated by accessing the data. Second, access to a user's data when it is segmented and constantly crossing borders would be impossible under a Mutual Legal Assistance Treaty, the potential availability of which played key a role in the *Microsoft* ruling.

The decision demonstrates that the Department of Justice is continuing to press arguments that did not win over the Second Circuit in the *Microsoft* case and underscores that the Second Circuit's approach may not hold sway elsewhere as other U.S. courts apply the SCA to companies' increasingly complex data-handling practices. The decision further muddles the status of cross-border data transfers, as U.S.-based cloud services providers may have a more difficult time representing whether data based in the European Union is exposed to U.S. government access. In addition to compounding the uncertainty of the legal landscape in this area, it increases the possibility that these issues may one day be headed to the U.S. Supreme Court.

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**.