

# SOCIALLY AWARE



2011 BEST LAW FIRM NEWSLETTER

## THE SOCIAL MEDIA LAW UPDATE

### IN THIS ISSUE

**Jerked Around? Did the FTC's "Jerk.com" Complaint Just Turn API Terms Into Federal Law?**  
Page 2

**Which Way Is *Aereo* Pointing? The Supreme Court Hears Arguments in Public Performance Copyright Case**  
Page 3

**The Umpire Strikes Back: European Court Rules That ISPs Can Be Forced to Block Pirate Websites**  
Page 5

**New Regulatory Guidance on Use of Social Media by Investment Advisers**  
Page 6

**Key Legal Concerns Raised by the Internet of Things**  
Page 7

**If You Host Videos on Your Website, Are You in Compliance With the Video Privacy Protection Act?**  
Page 11


### EDITORS

[John F. Delaney](#)  
[Gabriel E. Meister](#)  
[Aaron P. Rubin](#)

### CONTRIBUTORS

[Jay G. Baris](#)  
[Patrick J. Bernhardt](#)  
[Amy Collins](#)  
[John F. Delaney](#)  
[Adam J. Fleisher](#)  
[D. Reed Freeman, Jr.](#)  
[Alistair Maughan](#)  
[Whitney E. McCollum](#)  
[Julie O'Neill](#)  
[Craig B. Whitney](#)

### FOLLOW US

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

 [@MoFoSocMedia](#)

**MORRISON  
FOERSTER**



In this issue of *Socially Aware*, our Burton Award-winning guide to the law and business of social media, we analyze a groundbreaking FTC complaint alleging deceptive practices online that could turn website Terms of Use into federal law; we summarize a U.S. Supreme Court copyright case that could impact existing technologies and future technological innovation; we discuss a ruling from Europe's highest court that will aid copyright owners in the fight against illegal streaming sites; we report on new SEC guidance on social media use by investment advisers as it relates to testimonials; we take a look at the development of the Internet of Things and the many regulatory, privacy and security issues that go along with it; and we highlight a recent class action decision that potentially impacts any company that hosts videos on its website.

All this—plus a collection of thought-provoking statistics about digital music...

# JERKED AROUND? DID THE FTC'S "JERK.COM" COMPLAINT JUST TURN API TERMS INTO FEDERAL LAW?

By D. Reed Freeman, Jr., John F. Delaney and Adam J. Fleisher

The Federal Trade Commission's (FTC) [announcement](#) that it had filed a complaint against Jerk, LLC and its websites like "jerk.com" ("Jerk") looks at first glance like a run-of-the-mill FTC Section 5 enforcement action involving allegedly deceptive practices online. But hidden in the facts of Jerk's alleged misbehavior is a potentially significant expansion of the FTC's use of its deception authority.

In alleging that the violation of another company's terms can be part of a Section 5 violation in its own right, the FTC is breaking new ground.

According to the FTC's [complaint](#), Jerk allegedly led consumers to believe that the profiles on its websites were created by other users of the website. The company also allegedly sold "memberships" for \$30 a month that supposedly included features that would enable consumers to alter or delete their profiles, or to dispute false information in the profiles. Jerk also charged consumers a \$25 fee to email Jerk's customer service department, according to the FTC's complaint.

The FTC alleges that Jerk created between 73.4 million and 81.6 million unique consumer profiles primarily using information such as names and photos pulled from Facebook through application programming interfaces, or APIs. The complaint states that "[d]evelopers that use the Facebook platform must agree to Facebook's policies," such as obtaining users' explicit consent to share certain Facebook data and deleting information obtained from Facebook upon a consumer's request.

These alleged facts lend themselves to a straightforward violation of Section 5 of the FTC Act for deceptive acts or practices. Jerk allegedly represented that the content on its websites was user-generated, while it was in fact primarily pulled by Jerk from Facebook, making Jerk's representation false and misleading. The FTC, however, has gone well beyond this straightforward deceptiveness accusation here. Rather than simply alleging that Jerk's representations were false and misleading because the content was not generated by users, but rather from Facebook information, the complaint goes much further in alleging that Jerk "populated or caused to be populated the content on the vast majority of Jerk profiles by taking information from Facebook in violation of Facebook's policies...." The fact that the information was pulled from Facebook in violation of Facebook's policies does not seem to be material—let alone essential—to the deceptiveness allegation. Nonetheless, the complaint only alleges that "the representation [regarding the source of the content] was, and is, false or misleading" *after* stating that Jerk took information from Facebook in violation of Facebook's policies.

The FTC is breaking new ground here. *Jerk* is not the first time the FTC has brought a case based (in part) on an alleged violation of another company's terms or policies, but it is the first time the FTC has alleged that the violation of

another company's terms or policies can be part of a violation of Section 5 in its own right. In January 2000, the FTC brought a complaint against ReverseAuction.com ("Reverse Auction"), an auction website that was attempting to compete with eBay. The FTC's complaint was based, in part, on the allegation that Reverse Auction obtained and used email addresses and user IDs of eBay customers "after registering as an eBay user and agreeing to comply with and be bound by eBay's User Agreement." Like Facebook, eBay requires users to adhere to its applicable policies. In both the *Reverse Auction* and the *Jerk* matters, the FTC charged that the applicable website operator failed to comply with the policies that applied to such website operator's actions. The crucial difference between the cases is that, in *Reverse Auction*, the FTC's theory of deception was that Reverse Auction "represented to eBay" that Reverse Auction would comply with eBay's policies. In light of this precedent, *Jerk* is significant because the FTC's complaint alleges only that Jerk made false representations about the *source* of its information, not about its compliance with Facebook's policies *per se*. In other words, the FTC's complaint can be read to suggest that simply using information pulled from Facebook in violation of Facebook's policies is a deceptive act or practice, without any alleged misrepresentation to Facebook regarding the use of the information.

The FTC's *Jerk* action thus breaks away from *Reverse Auction* by characterizing actions inconsistent with a third party's policies as deceptive in their own right, as opposed to finding any *representation* regarding compliance with those policies to be deceptive. In that light, the FTC appears to have taken a case with ugly facts (including, allegedly, public availability on Jerk's websites of photos of children that had been tagged as "private" on Facebook) and leveraged such case to allege that noncompliance with Facebook's policies themselves is part of a violation

# digital music

## BY THE NUMBERS

### January 2012:

Digital music sales surpassed physical music sales for the first time ever.<sup>1</sup>

**54%** of smartphone users use music player apps.<sup>2</sup>

Smartphone users who use their phone's music player do so an average of **13** times a day.<sup>2</sup>

**40%** of music listeners download 5-10 songs per month.<sup>3</sup>

**70%** of music listeners pay to download music.<sup>3</sup>

**73%** of music listeners belong to a social music site.<sup>3</sup>

The global digital music industry's revenues grew by 4.3% in 2013 to **\$5.9 billion**.<sup>4</sup>

The number of paying subscribers to digital music services rose to **28 million** in 2013.<sup>4</sup>

**64%** of teens discover music using YouTube.<sup>5</sup>

of Section 5 in its own right. If the FTC continues to pursue this theory, it would essentially be turning Facebook's policies into "federal law," with compliance effectively enforced by the threat of Section 5 enforcement simply for using Facebook content in violation of Facebook's policies.

## WHICH WAY IS AEREO POINTING? THE SUPREME COURT HEARS ARGUMENTS IN PUBLIC PERFORMANCE COPYRIGHT CASE

By Craig B. Whitney and Whitney E. McCollum

In a case that could have a broad impact on how companies deliver content to consumers, the Supreme Court heard oral argument on April 22 in *American Broadcasting Companies, Inc. v. Aereo, Inc.* (No. 13-461). At issue is whether Aereo's service engages in public performances under the Copyright Act in transmitting broadcast television content to its subscribers' wired and wireless devices. While the Justices questioned both parties on a variety of issues, a clear focus for the Court was the potential impact of its decision on other technologies not at issue in this case.

### BACKGROUND

Aereo provides broadcast television streaming and recording services to its subscribers, who can watch selected programming on various Internet-connected devices, including televisions, mobile phones and tablets. Aereo provides its service through individual antennas that pick up local television broadcast signals and transmit those signals to a server where individual copies of programs embedded in such signals are created and saved to the directories of subscribers who want to view such programs. A subscriber can then watch the selected program nearly live (subject to a brief time-delay from the recording) or later from the recording. No two users share the same antenna at the same time, nor do any users share access to the same stored copy of a program.

In 2012, various broadcasting companies sued Aereo for copyright infringement in the Southern District of New York claiming, among other things, that Aereo's transmission of the plaintiffs' copyrighted content to Aereo's subscribers violated the copyright owners' exclusive right to publicly perform those works. That

SOURCES

1. <http://mashable.com/2012/07/24/music-sales-decline/>
2. <http://mashable.com/2013/07/10/sol-republic-music-infographic/>
3. <http://www.infographicsarchive.com/music/infographic-when-do-you-listen-to-music/>
4. <http://www.ifpi.org/downloads/Digital-Music-Report-2014.pdf>
5. <http://www.themusicvoid.com/2013/05/exclusive-infographic-how-people-are-consuming-music/>

public performance right, codified in the 1976 Copyright Act, includes (1) any performance at a place open to the public or any gathering with a substantial number of people outside the “normal circle of family and social acquaintances,” and (2) the transmission of a performance to the public whether or not those members of the public receive it in the same location and at the same time. This latter provision, commonly referred to as the Transmit Clause, was added to the Copyright Act by Congress in part to overturn prior Supreme Court precedent that had previously allowed cable companies to retransmit broadcast television signals without compensating the broadcaster.

The district court denied the broadcast companies’ preliminary injunction requests, finding that, based on Second Circuit precedent, Aereo’s transmissions were unlikely to constitute public performances. The Second Circuit affirmed the decision, relying on the court’s earlier decision in *Cartoon Network LP v. CSC Holdings, Inc.*, 536 F.3d 121 (2d Cir. 2008) (“*Cablevision*”), which found that a cable company’s remote-storage DVR system did not run afoul of the public performance right because each transmission was sent only to an individual user. The Second Circuit held that Aereo does not engage in public performances because, as in *Cablevision*, Aereo’s system makes unique copies of every recording, and each transmission of a program to a customer is generated from that customer’s unique copy.

Aereo has been sued by other broadcasters in other jurisdictions as well. The District of Massachusetts reached the same result as the Second Circuit, while the District of Utah came to the opposite conclusion. Further, both the D.C. District Court and the Central District of California have issued preliminary injunctions against FilmOn X, a company that offers a service similar to Aereo’s.

## **SUPREME COURT ORAL ARGUMENT**

A recurring theme during the oral argument was the impact the Court’s

decision would have on other technologies and industries. The Justices’ questions focused heavily on how their decision would affect other technologies, such as cloud computing and storage, how to balance technological innovation versus pure circumvention of copyright laws, and on how a decision against Aereo, were the Court to make such a decision, could be squared with the Second Circuit’s *Cablevision* opinion.

**A recurring theme during the oral argument was the impact the Court’s decision would have on other technologies and industries.**

### ***Effect on Other Technologies***

Justices Stephen Breyer and Sonia Sotomayor led off the discussion over the expected impact of the Court’s decision on other technologies. Justice Breyer plainly stated: “And then what disturbs me on the other side is I don’t understand what a decision for [Aereo] or against [Aereo] when I write it is going to do to all kinds of other technologies.” Justice Samuel Alito echoed this sentiment when he remarked: “I need to know how far the rationale that you want us to accept will go, and I need to understand, I think, what effect it will have on these other technologies.”

Neither party had a clear response that seemed to ease the Court’s concerns. The broadcasters sought to distinguish Aereo’s technology from cloud storage by pointing out that the cloud storage companies provide a “locker” for users to store their own rightfully owned content, and at times urged the Court to avoid the issue of cloud storage altogether—although the Court seemed unsure of how to accomplish that. Aereo stirred the pot by pointing out that a

decision finding that the performance of content stored by a third party constitutes a public performance could result in “potentially ruinous liability” for the cloud storage companies. Several other companies and technologies were identified by name during the arguments, including Netflix, Hulu and Roku.

While the early discussion seemed to focus on how the Court could find Aereo’s service a public performance without broader ramifications to the industry, most of the Court’s questions did not portend how the Court would ultimately rule. The Court, however, was undoubtedly cognizant that the decision could have an impact beyond the dispute at issue.

### ***Questioning the Merits of the Technology***

Chief Justice John Roberts questioned both parties on the technological aspects of Aereo’s service, first pointing out to the broadcasting companies that “[y]ou can go to Radio Shack and buy an antenna and a DVR or you can rent those facilities somewhere else from Aereo. They’ve—they’ve got an antenna. They’ll let you use it when you need it and they can, you know, record the stuff as well and let you pick it up when you need it.”

The broadcasters responded that allowing Aereo to take “a performance off the airwaves and transmit it to all the end-users” contradicts Congress’s specific intent when it enacted the Transmit Clause in response to cable providers’ prior transmissions of content without compensating the content owners.

Chief Justice Roberts then questioned Aereo as to the motive behind Aereo’s multi-antenna set-up, stating: “I mean, there’s no technological reason for you to have 10,000 dime-sized antenna, other than to get around copyright laws.” Justice Antonin Scalia followed up with, “Is there any reason you did it other than not to violate the copyright laws?”

According to Aereo, “All Aereo is doing is providing antennas and DVRs that enable consumers to do exactly what this

Court in *Sony [Corp. of America v. Universal City Studios, Inc.]* recognized they can do when they're in [their] home and they're moving the equipment . . .” Aereo distinguished itself from cable providers by the scope of content they provide (only content available over public airwaves) and how it is provided (upon a user’s initiation).

### ***Distinguishing Cablevision***

The Court also inquired as to how Aereo’s service differs, if at all, from the remote-storage DVR service provided in *Cablevision*. Justice Anthony Kennedy, in particular, seemed reluctant to reach a decision that effectively overruled *Cablevision*, even asking the broadcasting companies to “assume that *Cablevision* is our precedent.” The broadcasting companies attempted to distinguish Aereo’s service from the service in *Cablevision* by pointing out that the defendant in *Cablevision* paid royalties to carry programming in the first instance, whereas Aereo does not pay any royalties.

In any event, while the outcome of the case is as yet undetermined, it remains to be seen how any decision will impact other existing technologies and serve as a guide to innovators on crafting future technologies to avoid copyright infringement liability.

A decision is expected by the end of June.

## **THE UMPIRE STRIKES BACK: EUROPEAN COURT RULES THAT ISPS CAN BE FORCED TO BLOCK PIRATE WEBSITES**

By [Alistair Maughan](#)

On March 27, 2014, the highest court in the European Union—the Court of Justice for the European Union (CJEU)—decided that copyright owners

have the right to seek injunctions against Internet service providers (ISPs) requiring the ISPs to block access to pirate websites illegally streaming or making copyright material available for download.

The case arose out of a dispute in Austria between two movie companies and an Austrian ISP, UPC Telekabel Wien GmbH. The movie companies were concerned about access to an illegal streaming site, Kino.to, which was making copies of films such as *Vicky the Viking* and *The White Ribbon* available to its subscribers. The Austrian Supreme Court had asked the CJEU whether the movie companies were entitled under European law to seek an injunction against the ISP, not just against the illegal streaming site.

**Other copyright owners may be sharpening their swords for battle in the European courts.**

EU law allows holders of intellectual property rights to seek an injunction against any “intermediary” that provides services to third parties and, in doing so, helps them to infringe copyrighted works. The Austrian Supreme Court asked the CJEU for a ruling on whether ISPs in this position were considered to be an intermediary for the purposes of the European legislation.

The CJEU answered in the affirmative, finding that “a person who makes protected subject matter available to the public on a website without the agreement of the right holder is using the services of the business which provides internet access to persons accessing that subject matter.” So, in effect, an ISP such as UPC Telekabel that allows its customers to access protected subject matter made available

to the public on the Internet by a third party is an intermediary whose services are used to infringe copyright.

The ISP had argued that it could not be held responsible for the material on the streaming site because it had no business relationship or cooperation with the operators of the unauthorized streaming site and because there was no proof that any of the ISP’s subscribers had actually used Kino.to to access pirated films.

The CJEU had little sympathy for the ISP. It noted that EU copyright law does not require there to be a specific relationship between the person infringing copyright and the intermediary against whom an injunction might be sought, nor is it necessary to prove that end users have actually used the site at issue.

To some extent, the decision is not surprising—but it is important that it comes from Europe’s highest court. Previously, in a case in 2011 in the UK, the Motion Picture Association of America and various film studios sought an injunction against BT, a UK ISP, seeking to block access to a website that facilitated the sharing of materials infringing their copyrights.

In that case, the infringing website, [www.newzbin.co.uk](http://www.newzbin.co.uk), had originally been shut down following legal action but then immediately reappeared outside the UK and therefore not within the UK court’s jurisdiction. As a result, the claimants stepped up a level and applied for an injunction against BT as the ISP. BT argued that it did not have actual knowledge of the infringements, that it was a mere conduit and that an ISP was not obligated to monitor activity over its service.

In that case, the judge did not feel the need to refer the case to the CJEU and proceeded to grant the injunction. He held that BT had actual knowledge that some form of copyright infringement was happening in the sense that BT was aware that the service was being used to infringe—but it was not necessary to

show actual knowledge of any specific instances of infringement.

The Telekabel case goes further and is more broadly-based than the BT case—which will be of considerable comfort to copyright holders. The film industry has been seeking to enforce copyright rights against illegal streaming sites for some time, and the CJEU’s decision in this case is of significant importance in underlining that a key weapon in that fight—the ability to seek injunctions against the ISPs that facilitate access to online streaming sites—is valid.

Other copyright owners may be sharpening their swords for battle in the European courts.

## NEW REGULATORY GUIDANCE ON USE OF SOCIAL MEDIA BY INVESTMENT ADVISERS

By Jay G. Baris

Acknowledging the growing demand by consumers for information through social media, the Division of Investment Management set some ground rules on how investment advisers can use social media and publish advertisements featuring public commentary about them from social media sites.

Under the new rules, investment advisers may refer to commentary published in social media without violating the rule prohibiting publication of client “testimonials” if the content is independently produced and the adviser has no “material connection” with the independent social media site. While not a bright line in the sand, the distinction goes a long way to clear up this murky area of the law.

### BACKGROUND

The growing use of social media by consumers has created challenges for federal securities regulators, who

must enforce antifraud rules that were written at a time when the prevailing technology was the newspaper.

Section 206 of the Investment Advisers Act of 1940 (“Advisers Act”) contains broad antifraud provisions that apply to advisers. Rule 206(4)-1(a)(1) under the Advisers Act defines fraud to include “any advertisement which refers, directly or indirectly, to any testimonial of any kind concerning the investment adviser or concerning any advice, analysis, report or other service” provided by the adviser. This is the so-called “testimonial rule.” In a 1985 no-action letter, the Division of Investment Management staff said that the basis of the prohibition is that a “testimonial may give rise to a fraudulent or deceptive implication, or mistaken inference, that the experience of the person giving the testimonial is typical of the experience of the adviser’s clients.”

**The growing use of social media by consumers has created challenges for federal securities regulators, who must enforce antifraud rules that were written at a time when the prevailing technology was the newspaper.**

While the SEC’s rules do not define the term “testimonial,” the SEC’s staff has indicated that public commentary made by a client endorsing an investment adviser, or a statement made by a third party about a client’s experience with the adviser, may be a testimonial for this purpose. And, as the guidance notes, whether public commentary on a social media site constitutes a testimonial depends on the facts and

circumstances relating to the statement.

In the age of social media, this decades-old rule presents enormous compliance challenges for advisers whose clients rely on social media.

Over the years, the staff, through the “no-action” process, has provided limited guidance on what constitutes a testimonial. For example, the staff has said that publication of an article by an unbiased third party regarding an adviser’s performance, unless it includes a statement of a client’s experience with the adviser, or an endorsement of the adviser, would not violate the testimonial rule. The staff has used this concept as the basis for its current guidance.

### GUIDANCE

*Third-party commentary.* The staff attempted to draw a line between endorsements and legitimate third-party commentary:

- Advisers may not publish public commentary on their website that is an explicit or implicit statement of a client’s experience with the adviser.
- Commentary posted directly on the adviser’s website, blog, or social media site that touts the adviser’s services are prohibited testimonials.
- Advisers won’t necessarily violate the testimonial rule if they publish commentary originating from an independent social media site on their own websites or social media sites, provided:
  - The independent social media site provides content that is independent of the investment adviser or its representative;
  - There is no material connection between the independent social media site and the investment adviser or its representative that would “call into question the independence” of the independent social media site or its commentary; and

- The investment adviser or representative publishes all of the unedited comments appearing on the independent social media site regarding the adviser or representative.
- Content is not “independent” if the adviser or its representative had a hand in authoring the commentary, directly or indirectly. For example, paying a client (or offering a discount to a client) for saying nice things would implicate the testimonial rule.
- Advisers may not use testimonials from independent social media sites that directly or indirectly emphasize commentary favorable to the adviser, or downplay unfavorable commentary.
- Advisers may publish commentary from an independent social media site that includes a mathematical average of the public commentary—for example, based on a ratings system that is not pre-ordained to benefit the adviser.

***Investment adviser advertisements on independent social media sites.***

- Investment advisers may advertise on an independent social media site, provided that it is readily apparent that the advertisement is separate from the public commentary, and that the receipt of advertising did not influence the selection of public commentary for publication.

***Reference to independent social media site commentary in non-social media advertisements.***

- In print, TV and radio ads, advisers *may* refer to the fact that third-party social media sites feature public commentary about the adviser, but they *may not* publish any actual testimonials without implicating the testimonial rule.

***Client lists on social media sites.***

- Simply identifying contacts or friends on a social media site

by itself does not implicate the testimonial rule, as long as they are not grouped in a way that suggests that they endorse the investment adviser.

***Fan and community pages.***

- A third party’s creation and operation of unconnected community or fan pages generally would not implicate the testimonial rule. However, the staff strongly cautions advisers and their employees that publishing content from those sites or directing user traffic to those sites if they do not meet the *no material connection* and *independence* conditions described above may implicate the testimonial rule.

**OUR TAKE**

The Division of Investment Management’s approach to regulating the use of social media by advisers differs markedly from the approach adopted by FINRA for broker-dealers. While both regulators focus on the substance of the communication, rather than the format, the differences arise primarily from the nature of the regulated entity and the starting point of regulation.

For example, the Division of Investment Management focuses almost exclusively on adequacy of compliance programs, and whether a particular use of social media involves a prohibited “testimonial,” a concept largely absent from regulation of broker-dealers. On the other hand, FINRA focuses on suitability of a recommendation and whether a particular communication requires advance compliance approval. Both approaches require caution when a regulated entity publishes or relies on third-party content.

The Division of Investment Management’s guidance moves the ball forward, and will provide a starting point for chief compliance officers who are struggling to get their arms around advisers’ use of social media. It may also provide an opportunity

for advisers to revisit their procedures for monitoring advertising. While the guidance provides some relief for advisers who now have a better idea of the limitations to which they are subject, it also provides some compliance challenges, especially when advisers and their representatives make use of fast-paced social media to advertise.

**KEY LEGAL CONCERNS RAISED BY THE INTERNET OF THINGS**

By Amy Collins, Adam J. Fleisher, D. Reed Freeman, Jr. and Alistair Maughan

Cisco estimates that 25 billion devices will be connected in the Internet of Things (“IoT”) by 2015, and 50 billion by 2020. Analyst firm IDC makes an even bolder prediction: 212 billion connected devices by 2020. This massive increase in connectedness will drive a wave of innovation and could generate up to *\$19 trillion* in savings over the next decade, according to Cisco’s estimates.

**THE ISSUES**

In the new world of the IoT, the problem is, in many cases, the old problem squared. Contractually, the explosion of devices and platforms will create the need for a web of inter-dependent providers and alliances, with consequent issues such as liability, intellectual property ownership and compliance with consumer protection regulations.

The IoT also raises a number of data-related legal and ethical issues, associated primarily with the collection and use of the vast quantities of data processed as a result. The IoT will enable the creation and sharing of massive new reservoirs of data about individuals’ habits, behavior

and personal preferences, thereby reinforcing global society's reliance on data, and making the laws and regulations which protect data privacy and limit data use even more fundamentally important.

Regulatory bodies, including the Federal Trade Commission (FTC) in the United States and the European Commission ("EU Commission") in the European Union, are in particular turning their attention to the potential privacy and security issues that the IoT undoubtedly presents.

In 2013, the EU Commission published a report on the results of its public consultation on the IoT, along with a series of accompanying fact sheets (together, the "Report"), highlighting that "the development towards an IoT is likely to give rise to a number of ethical issues and debates in society, many of which have already surfaced in connection with the current Internet and ICT in general, such as loss of trust, violations of privacy, misuse of data, ambiguity of copyright, digital divide, identity theft, problems of control and of access to information and freedom of speech and expression. However, in IoT, many of these problems gain a new dimension in light of the increased complexity."

At the top of the list of issues facing law and policy makers in this area are the following:

- *Loss of privacy and data protection.* The difficulties of complying with the principles of privacy and data protection, such as informed consent and data minimisation, are likely to grow considerably. As the EU Commission has stated in its Report, "It can reasonably be forecast, that if IoT is not designed from the start to meet suitable detailed requirements that underpin the right of deletion, right to be forgotten, data portability, privacy and data protection principles, then we will face the problem of misuse of IoT systems and consumer detriment."
- *Autonomous communication.* One of the most significant IoT-related data privacy risks stems from the fact that devices are able, and intended, to communicate with each other and transfer data autonomously. With applications operating in the background, individuals may not be aware of any processing taking place, and the ability for data subjects to exercise their data privacy/protection rights may therefore be substantially impaired.
- *Traceability and unlawful profiling.* In 2013, researchers at Cambridge University demonstrated that incredibly accurate estimates of race, age, IQ, sexuality, personality, substance use and political views could be inferred from automated analysis of their Facebook "Likes" alone. Similarly, although the objects within the IoT might individually collect seemingly innocuous fragments of data, when that data is collated and analysed, it could potentially expose far more than intended by the individual to whom it relates, and indeed more than those Facebook Likes. The data collected, in combination with data from other sources, may reveal information on individuals' habits, locations, interests and other personal information and preferences, resulting in increased user traceability and profiling. This in turn increases the risk of authentication issues, failure of electronic identification and identity theft.
- *Malicious attacks.* The IoT provides hackers with more vulnerabilities to exploit and creates significant security risks. Such risks could take a variety of forms, depending on the nature of the data and device in question. In the context of e-health, the collection and rapid exchange of sensitive personal information in an interconnected and open environment not only increases risks in respect of patient confidentiality, but also has the far more alarming

In the new world of the Internet of Things, the problem is, in many cases, the old problem squared.

potential to endanger life. Take, for example, the remote programming of a heart pacemaker, or a drug dispenser configured to administer medication in response to a patient's condition. A system failure or more sinister malicious attack on such device could have dire consequences. Regarding energy, hackers could target smart meters to cause major blackouts, and, regarding home security, little imagination is required to envision the potential effects of a system failure or malicious attack. Such threats to security and privacy vary considerably and the breadth of challenges presented means that a one-size-fits-all approach to policy and/or regulation is unlikely to work.

- *Repurposing of data.* The risk that data may be used for purposes in addition to or other than those originally contemplated and specified by the data subject becomes even greater in the IoT. Repurposing of data may be contemplated even before data collection begins. For example, regulatory bodies, insurance companies and advertising agencies, among others, may seek access to data collected by others. Controls are needed to ensure that such data is only used in the manner consented to by the data subject. While an individual might be happy for his fridge to know how many pizzas he eats each week, he might be less comfortable if he knew that that information was being passed on to his health insurance provider.
- *User lock-in.* As is the case for existing technologies, the IoT increases the risk that consumers may become



locked-in to a specific IoT service provider, thereby impeding their ability to retain control over their data and their right to move from one provider to another.

- *Applicable law.* With IoT devices, systems, users and service providers located in any number of jurisdictions, the global nature of the IoT means that various national laws may be applicable, each providing different levels of protection. This may give rise to questions of conflict, difficulties in enforcement and confusion among consumers.

## THE FUTURE REGULATORY LANDSCAPE

Looking ahead, the question is what approach should be taken by law and policy makers to address these issues?

In response to the EU Commission's public consultation, a large number of industry players questioned the legitimacy and appropriateness of public intervention in an area which, although it has come a long way since 1999, is still arguably in its infancy. These stakeholders maintained that the existing legal framework, including data privacy, competition, safety and environmental legislation, is sufficient to protect end users' interests, and inappropriate governance at this stage may stifle investment and innovation. Conversely, the majority of individual respondents argued that economic considerations should take a back seat to the fundamental issues of privacy and security. They contended that specific rules should be developed and enforced to protect end users and to control the development of IoT technologies and markets.

Keeping in mind (1) the international dimension of the IoT, (2) the resulting need for interoperability, (3) the importance of a harmonised internal market and (4) the universality of the fundamental rights to privacy and data protection, the EU Commission commented that it would be inadvisable to allow divergence at a member state level of the law and methodologies in

this area. That is, of course, a statement of the obvious.

But avoiding legal and regulatory fragmentation across key jurisdictions is a forlorn hope. Regulatory differences will occur, just as it has happened with the cloud, with data privacy and with many other regulated technologies. The truth is that governments just don't act quickly enough to keep up with new technology, and don't have the power or inclination to agree completely on harmonized legal and regulatory approaches to new technologies.

Looking ahead, the question is what approach should be taken by law and policy makers to address issues presented by the Internet of Things?

## EUROPE

The EU's draft Data Protection Regulation (the "Draft Regulation"), which is likely to be adopted in summer 2014, will go some way to provide the necessary harmonisation—at least within Europe. The Draft Regulation will replace the existing Data Protection Directive 95/46/EC and will have direct effect, not only to organizations established in the EU/EEA, but also to other organizations that collect and process EU/EEA residents' personal data. (For more on the changes proposed by the draft Regulation, see our January 2012 alert [A New Chapter in European Data Protection: Commissioner Reding Publishes Long-Awaited Draft Data Protection Regulation.](#)) Some of the measures that we might expect to see as a result of these developments are as follows:

- *Privacy by design and default.* In its Report, the EU Commission noted that individuals' privacy, data

protection and security rights are often not considered at the outset of the design process, and it is unlikely that they will be properly addressed by the market without regulation. The Draft Regulation provides that, "having regard to the state of the art and the cost of implementation," the data controller must, "both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures in such a way that the processing will ensure the protection of the rights of the data subject." In addition, the data controller must "implement mechanisms for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing, and are not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage." In particular, those mechanisms must "ensure that by default, personal data are not made accessible to an indefinite number of individuals."

- *Consent.* In its Report, the EU Commission emphasised that mechanisms are needed to ensure that no unwanted processing of personal data takes place and that individuals are informed of the processing, its purposes, the identity of the processor and how to exercise their rights. The Draft Regulation defines consent as "any freely given, specific, informed and explicit indication" of an individual's wishes, and can be expressed in the form of a statement or a clear affirmative action that signifies agreement to the processing. Tacit or implied consent could be valid: however, the preamble to the Draft Regulation confirms that silence or inactivity would not suffice. It remains to be seen exactly how these requirements will be met where applications in the IoT act autonomously or "behind the scenes."

- *Measures based on profiling.* As noted above, the IoT gives rise to serious concerns in terms of profiling and user traceability. The Draft Regulation sets out the circumstances in which such profiling, “which is based solely on automated processing intended to evaluate certain personal aspects...or to analyse or predict in particular the natural person’s performance at work, economic situation, location, health, personal preferences, reliability or behaviour,” would be considered lawful. This includes where the data subject has consented, or where, in the context of the performance of a contract, suitable measures to safeguard the data subjects’ legitimate interests have been adduced.
- *Privacy policies.* In its Report, the EU Commission advised that privacy policies that can be pushed or built into IoT objects should be adopted, with appropriate mechanisms to ensure data privacy. It noted, however, that the technical challenge here is how to enable objects with limited processing power and/or memory to receive and respect such policies. Given the sheer number of IoT devices, the uniformity of such policies should also be considered.
- *Enforcement and sanction.* The EU Commission also highlighted a need to strengthen and clarify the powers of data protection authorities to ensure consistent monitoring and enforcement of applicable law. Amongst other things, the Draft Regulation introduces significant sanctions for violations of data privacy obligations, including fines of up to 5% of annual worldwide turnover, or €100 million, whichever is greater. The Draft Regulation also extends the concept of mandatory personal data breach notifications to all areas of personal data processing.

In its Report, the EU Commission acknowledged that, because the “IoT is a special case and more of a vision rather than a concrete technology, we understand that it is complex to properly define all the requirements yet.” While

the Draft Regulation goes some way to address the issues to which the IoT gives rise, it remains to be seen exactly how the law and policy in this area will develop as the IoT itself evolves.

## UNITED STATES

On the other side of the Atlantic, privacy and data security in the IoT is also firmly on the agenda. Regulators in the United States—particularly the FTC—seem to be focused on the same privacy and security issues as their EU counterparts. In terms of how these concerns manifest in a regulatory context, the FTC is most likely going to rely upon its standard notice and choice framework on the privacy side, and its position that the lack of reasonable security measures to protect consumer data may be an unfair or deceptive act or practice under Section 5 of the FTC Act. To that end, future FTC enforcement is most likely to focus in particular on two main areas when it comes to IoT: (1) providing notice and choice when a networked device is not consumer-facing; and (2) how to ensure that devices that are part of the IoT ensure reasonably data security.

We have various indicators of why the FTC will focus on these particular issues:

- *Workshop on the Internet of Things.* The FTC held a workshop examining privacy and security issues surrounding the IoT in November 2013. The workshop focused on those issues related to increased connectivity for consumers, both in the home (including home automation, smart home appliances and connected devices), and when consumers are on the move (including health and fitness devices, personal devices and cars). The FTC will publish a best practices report about the IoT at some time in 2014. The key themes articulated by the FTC at the workshop itself were: (1) the risks to consumer privacy from the collection, analysis, and unexpected uses of large amounts of data about consumers; (2) the possibility that traditional notice and consent frameworks will

not be sufficient to inform consumers of how their personal data is being used; and (3) the data security risks of interconnected objects. In her opening remarks at the workshop, FTC Chairwoman Ramirez emphasized that “as the boundaries between the virtual and physical worlds disappear,” there still needs to be some way to give consumers notice and choice about the information collected about them, and how it is used, even if the device has no user interface.

- *TRENDnet Enforcement Action.* The FTC brought its first-ever IoT case in December 2013 against TRENDnet, the maker of a surveillance camera system with a range of uses from home security to baby monitoring. The company’s cameras had a faulty software configuration that left them open to online viewing, and in some instances listening, by anyone with the cameras’ Internet address. As a result, nearly 700 live camera feeds were accessed by a hacker. The FTC’s complaint alleged that the company’s failure to reasonably secure its cameras against unauthorized access was an unfair and deceptive act and practice under Section 5 because the company represented it had reasonable security measures in place when it in fact did not. This type of case is fairly standard for an FTC data security case; what distinguishes it is that, as the FTC explained, the product involved falls under the IoT umbrella because it is an *everyday product* with interconnectivity to the Internet and other mobile devices.
- *FTC Commissioners’ speeches regarding the IoT.* Two FTC Commissioners have spoken recently about the policy and regulatory implications of the IoT, which provides some sense of future enforcement priorities and the contours of the regulatory framework:
  - In February 2014, Commissioner Julie Brill spoke on *The Internet of Things: Building Trust to*

*Maximize Consumer Benefits.* Commissioner Brill tied the IoT to another major policy concern of the FTC—“big data.” She cited Cisco’s estimate that there will be 25 billion Internet-connected devices by 2015, and noted that, by the end of this decade, 40% of data could come from connected devices. As a result, her main concern is that data from devices—that consumers might not even know are actually connected to the Internet—can be combined with existing troves of data to make it even easier to make sensitive predictions about consumers, such as those involving their sexual orientation, health conditions, religion and race.

- In October 2013, Commissioner Maureen K. Ohlhausen spoke on *The Internet of Things and the FTC: Does Innovation Require Intervention?* While the Commissioner emphasized the potential privacy and data security risks posed by greater interconnectedness of devices, her remarks focused more on the transformative potential, and the human benefits, of the IoT. To that end, she sees the role of the FTC as ensuring that businesses have the freedom to experiment and innovate so that the benefits of this technological advance can be realized. Thus, while the FTC should use its traditional deception and unfairness authority to stop consumer harms arising from Internet-connected devices, the FTC should also focus on consumer tips and best practices relating to the IoT.

Finally, a number of U.S. states have proposed legislation on the 2014 docket that is intended to increase privacy protection for consumers. At a federal level, several bills are also in the process of going through Congress. These include the [Black Box Privacy Protection Act](#) (which would (1) prohibit the sale of

automobiles equipped with event data recorders, unless consumers are able to control the recording of such data, and (2) require that any data so recorded would be considered the property of the vehicle owner) and the [We Are Watching You Act](#) (which would provide for notification of consumers before a video service collects visual or aural information from the viewing area).

## CONCLUSION

Given the tremendous growth of the Internet of Things, and the predictions that it will continue to grow exponentially, it is likely that the lawmakers and policymakers will play a considerable role in shaping the development of the IoT in the next few years.

The regulatory framework within which the IoT operates is an important factor to consider for technology companies seeking to harness the power of machine-to-machine (M2M) connectivity. The key issues seem likely to be whether the regulators can work fast enough to keep up with what the technology is capable of doing, and whether law and policy in key markets around the world is harmonized—at least in key parts—to ensure that the IoT is allowed to develop in a way supported by applicable laws, not handicapped by fragmented and contradictory legislation.

Businesses implementing M2M-based solutions will clearly need to examine their data privacy policies and approaches to data security in order to anticipate and meet the challenges presented by the IoT.

As noted above, Cisco is predicting that there will be 50 billion connected devices by 2020. Or, to put it another way, “Today there are more things connected to the Internet than there are people in the world. In the very near future, pretty much everything you can imagine will wake up.” [Numerous articles note](#) the diversity of devices that can and will be connected in the near future, from cars to parking meters to home thermostats, which makes it seem as if we are at the beginning of an entirely new chapter in the history of the Internet.

For more information regarding IoT, see our [article](#) examining the development of, and practical challenges facing businesses implementing, IoT solutions.

# IF YOU HOST VIDEOS ON YOUR WEBSITE, ARE YOU IN COMPLIANCE WITH THE VIDEO PRIVACY PROTECTION ACT?

By [D. Reed Freeman, Jr.](#), [Julie O’Neill](#) and [Patrick J. Bernhardt](#)

In a much anticipated [decision in the class action \*In re Hulu Privacy Litigation\*](#), U.S. Magistrate Judge Laurel Beeler of the U.S. District Court for the Northern District of California has shed new light on the meaning of “personally identifiable information” (PII) under the Video Privacy Protection Act (VPPA). This has important implications for companies that host videos on their websites and integrate their services with social media companies or web analytics service providers.

The key issue for the court was whether the disclosures of the video titles were tied to specific identified persons, such that they constituted prohibited disclosures of PII under the VPPA.

The court held on summary judgment that the transmission to a third party of unique user IDs, *in and of themselves*, along with video viewing history, does not constitute disclosure of PII under the VPPA.

In reaching its conclusion, the court

distinguished between anonymous IDs that Hulu, LLC provided to the audience metrics company comScore, Inc. (which the court held were not PII) and a social networking service's user IDs that Hulu provided to the social networking service (as to which the court held there were material issues of fact with respect to whether they could permit the identification of specific persons and thus be PII).

The court granted Hulu's motion for summary judgment with respect to the comScore disclosures but not with respect to the social networking service disclosures.

## KEY POINTS

The court's decision shows that, when determining whether unique IDs associated with consumers' online video viewing history are PII regulated by the VPPA, context matters.

In particular, companies that transmit such information should be aware of several key points:

- First, the decision declined to impose VPPA liability for the disclosure of unique user IDs associated with video viewing history, where such IDs did not identify specific persons and where the record revealed only a hypothetical ability to correlate unique user IDs to specific persons but no evidence that it actually happened.
- Second, the decision makes clear that companies should be mindful of the context in which they share unique user IDs with third parties, particularly with respect to whether the IDs permit the recipient or another party to identify specific persons, either directly or through information to which they already have access.
- Third, the decision highlights the potential danger for companies that integrate social media plug-ins or other functionality on web pages where consumers watch videos.

Companies providing online video services should consider taking steps to ensure that: (1) cookies and other data transmitted to another entity, such as a user ID that is matched with the video provider's user ID for the same person, do not permit identification of specific individuals; and (2) video viewing history is not shared unintentionally, such as through a referrer URL that is transmitted during a standard browser request.

- Finally, the decision highlights other important questions of fact that may exist when evaluating VPPA exposure, including whether the disclosing party had knowledge of the disclosure and whether the consumer consented to it.

## BACKGROUND

With limited exceptions, the VPPA imposes liability—including liquidated damages of up to \$2,500 per incident—on a video tape service provider that knowingly discloses, to any person, PII concerning any consumer of the video tape service provider. Liability extends to companies that provide online video services, such as Hulu, and the definition of PII includes “information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider.”

In this case, the plaintiffs alleged that Hulu wrongfully disclosed its users' video viewing history to comScore and a social networking service. comScore had provided Hulu with audience metric data about Hulu's users, and the social networking service had provided social networking features through placement of its “Like” button on Hulu's video watch pages. Each company received different data from Hulu during the delivery of its services. Among other data, comScore received unique numerical Hulu User IDs and comScore User IDs, while the social networking service had access to its own first-party cookies containing its own unique user IDs. Each company also received the title of the video watched,

either as a parameter in a set of data transmitted or in the referrer URL of the page on which the user viewed the video.

## ASSESSING THE LINK BETWEEN USER IDS AND SPECIFIC PERSONS

In its decision, the court addressed three different disclosures by Hulu:

- the disclosure to comScore of watch pages and Hulu User IDs;
- the disclosure to comScore of the comScore User ID cookies; and
- the disclosure to the social networking service of watch pages and the social networking service's cookies.

The key issue for the court was whether the disclosures of the video titles were tied to specific identified persons, such that they constituted prohibited disclosures of PII under the VPPA. The court stated that “the statute, the legislative history, and the case law do not require a name, [but] instead require the identification of a specific person tied to a specific transaction . . . .” Providing further explanation, the court stated that “a unique anonymized ID alone is not PII but context could render it not anonymous and the equivalent of the identification of a specific person.” In other words, context matters insofar as the circumstances link the unique user IDs to specific persons.

In applying this reasoning, the court held that Hulu's disclosure to comScore of watch pages and Hulu User IDs did not constitute disclosure of PII: despite the fact that comScore could have used the Hulu User IDs to access Hulu users' profile pages and obtain their names, there was no evidence that it did so, and there was thus no disclosure of PII for purposes of the VPPA.

The court next addressed Hulu's disclosure to comScore of the comScore User ID cookies. The court explained that, although the comScore User IDs permitted comScore to conduct “substantial tracking that reveals a lot of information about a person,” the

disclosure did not violate the VPPA because the tracking did not reveal “an identified person and his video watching.”

On the other hand, the court suggested that disclosure of the social networking service’s own, first-party user IDs to the social networking service itself, together with video viewing history, may constitute disclosure of PII under the VPPA. The court noted that “[t]he Facebook User ID is more than a unique, anonymous identifier. It personally identifies a Facebook user. That it is a string of numbers and letters does not alter the conclusion.” In addition, the court emphasized that “a Facebook user—even one using a nickname—generally is an identified person on a social network platform” and that “[the Facebook User ID] identifies the Hulu user’s actual identity on Facebook.” Therefore, the court denied Hulu’s motion for summary judgment with respect to its disclosures to the social networking service.

The decision with respect to the social networking service highlights the risk posed by integrations with social media companies on websites that host video services. Such integrations may cause a cookie or other data to be sent from a user’s browser without any affirmative action by the user, which could permit the social media company to identify

a specific person and his or her video watch history—and thus trigger VPPA liability, although the court declined to make a decision on this aspect at this stage of the proceedings.

In practical terms, this risk means that companies providing online video services should take steps to ensure that: (1) cookies and other data transmitted to another entity, such as a user ID that is matched with the video provider’s user ID for the same person, do not permit identification of specific individuals; and (2) video viewing history is not shared unintentionally, such as through a referrer URL that is transmitted during a standard browser request.

### **OTHER POTENTIAL LIMITATIONS UNDER THE VPPA: “KNOWING” DISCLOSURE AND USER CONSENT**

The court ruled that material issues of fact remained regarding whether Hulu disclosed the social networking service’s user IDs knowingly and without user consent. The court stated that “[o]ther cases involving violations of privacy statutes show that in the context of a disclosure of private information, ‘knowingly’ means consciousness of transmitting the private information. It does not mean merely transmitting the code.” Thus, the court stated that “if [Hulu] knew what [the social networking

service’s cookies] contained and knew that it was transmitting PII . . . then Hulu is liable under the VPPA.” The court did not, however, grant summary judgment to Hulu based simply on the fact that Hulu’s servers could not read the social networking service’s cookies. Rather, the court held that other evidence may show that Hulu knew that the social networking service was receiving its own first-party user IDs within its cookies and was reading them together with video viewing history.

Finally, the court also denied Hulu’s motion for summary judgment with respect to whether consumers had given consent to any disclosures through their acceptance of the social networking service’s privacy policy or whether such “consent,” if found, was sufficient under the VPPA.

### **CONCLUSION**

In light of the court’s decision, companies that—without affected individuals’ VPPA-compliant consent—disclose any type of identifier, together with video viewing history, to any other person or company should pay very close attention to exactly what information they transmit and whether it could be used by the recipient to identify specific individuals.

If you wish to receive a free subscription to our Socially Aware newsletter, please send a request via email to [sociallyaware@mofocom](mailto:sociallyaware@mofocom). We also cover social media-related business and legal developments on our Socially Aware blog, located at [www.sociallyawareblog.com](http://www.sociallyawareblog.com).

For breaking news related to social media law, follow us on Twitter [@MoFoSocMedia](https://twitter.com/MoFoSocMedia). To review earlier issues of Socially Aware, visit us at [www.mofocom/sociallyaware](http://www.mofocom/sociallyaware).

We are Morrison & Foerster — a global firm of exceptional credentials. With more than 1,000 lawyers in 17 offices in key technology and financial centers in the United States, Europe and Asia, our clients include some of the largest financial institutions, investment banks, and Fortune 100, technology and life science companies. We’ve been included on *The American Lawyer’s* A-List for 10 straight years, and *Chambers Global* named MoFo its 2013 USA Law Firm of the Year. Our lawyers are committed to achieving innovative and business-minded results for our clients, while preserving the differences that make us stronger

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