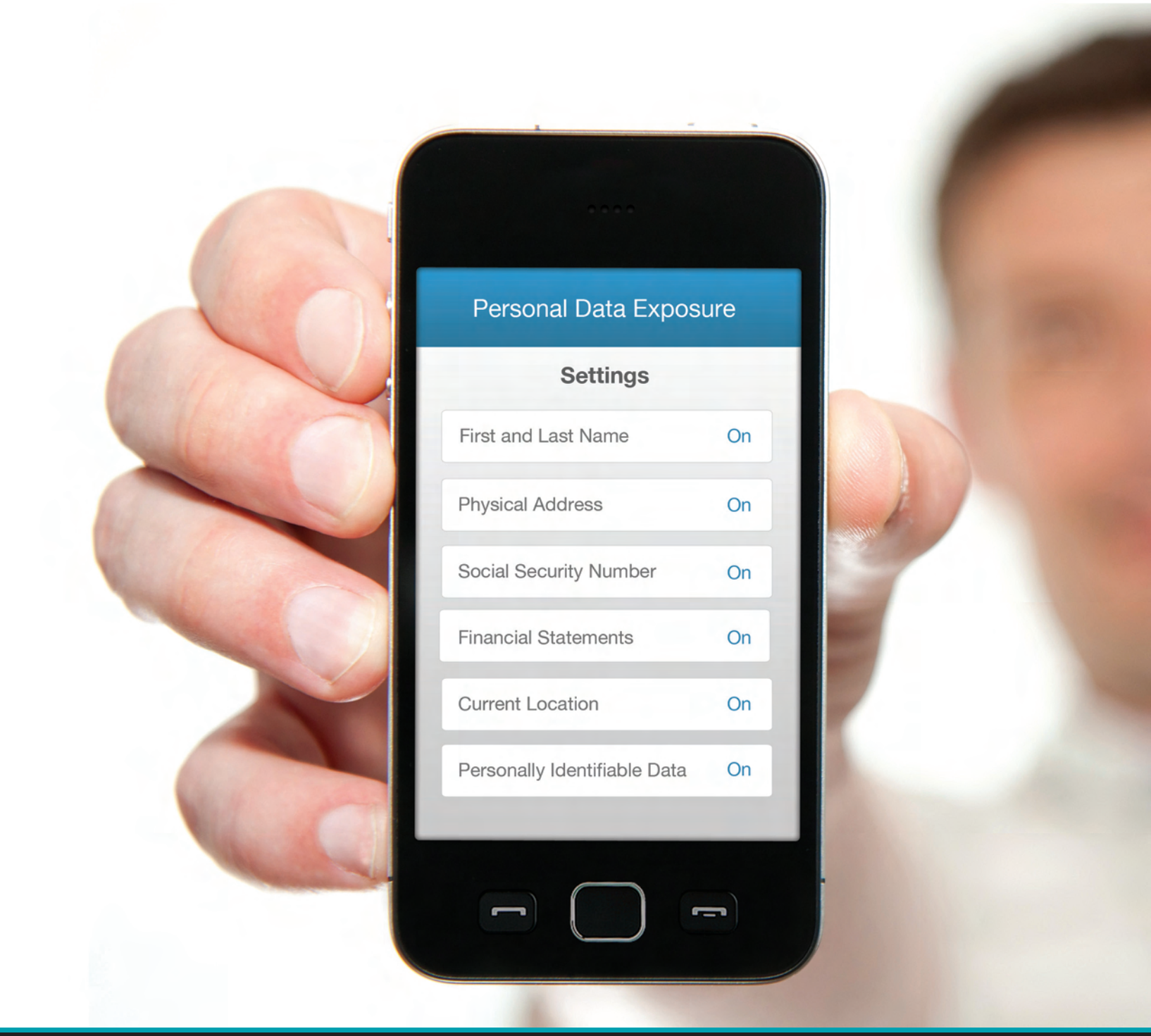
M/E INSIGHTS

ADVANCED MEDIA WINTER/SPRING 2011



AMEC
THE ASSOCIATION OF MEDIA & ENTERTANMENT COUNSEL

GUEST EDITOR
Alan Friel
friel@wildman.com

EDITOR-IN-CHIEF
Drew Wheeler
AMECInsights@gmail.com

MANAGING EDITOR
Julia Harris
Harrisjulia56@gmail.com

DESIGN EDITOR
Elena Kapintcheva
elena@kapincheva.com

FOR MEMBERSHIP AND SPONSORSHIP OPPORTUNITIES, CONTACT
Serra Aladag
Serra@theamec.com

FOR ADVERTISING OPPORTUNITIES AND REPRINT INFORMATION, CONTACT
Drew Wheeler
AMECInsights@gmail.com

ADVISORY BOARDS

THE ASSOCIATION OF MEDIA AND ENTERTAINMENT COUNSEL
5225 Wilshire Blvd. #417
Los Angeles, CA 90036
p: 310.432.0507
f: 310.277.1980
www.theamec.com

EXECUTIVE DIRECTOR
Serra Aladag
serra@theamec.com

CONTENT

LETTER FROM THE GUEST EDITOR

DISRUPTIVE TECHNOLOGY PRESENTS CHALLENGES AND OPPORTUNITIES FOR MEDIA AND ENTERTAINMENT COMPANIES—AND THE LAWYERS THAT ADVISE THEM...

Alan L. Friel
Partner, Wildman, Harrold, Allen and Dixon LLP
IAPP Certified Information Privacy Professional

I am pleased to be invited back this year to guest edit another issue of *M/E Insights.* Last year, I predicted increased enforcement by the Federal Trade Commission ("FTC") with respect to the use of social and online media to promote products and services under the FTC's then-recently-revised *Guides Concerning the Use of Endorsements and Testimonial in Advertising,* and warned you to expect greater federal attention to issues involving consumer data privacy and security. As many of the articles in this edition demonstrate, both forecasts have come to pass. In addition, the class action plaintiffs' bar has discovered the "privacy issue," and lawsuits related to companies' online and mobile privacy policies and practices abound. Also, the evolution of technology has continued to bring even more new ways to interact with media, and with that, concerns regarding the balance of consumer choice (and rights) with copyright owners' legitimate protection.

Firstly, addressing the big picture of how to deal with the disruptive effects of digital technology, we have two persuasive articles taking somewhat different approaches to the role of copyright in the digital era:

In his piece *Copyright and Free Speech in the Age of Digital Piracy,* Michael Fricklas, the General Counsel of Viacom, discusses the challenges the content industry faces from digital piracy and suggests a balance between free speech and fair use when protecting the copyright interests of content owners. Robert Tercek, however, warns that tougher laws and practices that try to protect content owners and their current business models (and distribution windows!) are the wrong approach. In *Tougher Copyright Laws Won't Solve Big Media's Internet Problem, But They Will Stifle Innovation,* Tercek urges traditional media companies to embrace disruptive technology, distributing their content via media and models that offer maximum consumer flexibility and choice. Fricklas' and Tercek's arguments are not necessarily incompatible with each other, but their perspectives clearly differ. Both articles are part of an important discussion that continues as digital media evolves and both technology and content companies (and their legal advisors) must adapt to the ways the digital ecosystem changes the way content will be used and distributed.

pg. 20 to 27 — **ONLINE BEHAVIORAL ADVERTISING LITIGATION AND PROPOSED LEGISLATION:** LESSONS FOR ONLINE PUBLISHERS AND ADVERTISERS

pg. 28 to 31 — **RECENT FTC ENFORCEMENT ACTIONS INVOLVING ENDORSEMENTS, PRIVACY AND DATA SECURITY**

pg. 32 to 36 — **APP-ENDECTOMY:** REMOVING THE MYSTERY FROM THE APP ECOSYSTEM

pg. 37 to 39 — **SOCIAL NETWORKING:** WHY CAN'T WE BE FRIENDS?

James Taylor and Jill Westmoreland summarize the FTC's recent enforcement actions regarding endorsements, privacy, and data security, explain what lawyers should learn from them, and provide a helpful list of resources to help companies comply with applicable laws and best practices. Dominique Shelton's article surveys the litigation and legislative landscape regarding online behavioral advertising (the tracking of consumer's online activates to build behavioral profiles enabling the targeting of contextually relevant ads), and offers suggestions on how to avoid becoming a defendant—and how to defend an action if sued. Nick Graham, a lawyer in the United Kingdom, discusses the impact of Europe's new rule requiring consumer consent before enabling website cookies or other tracking technology stored on a user's computer or mobile device—reminding us that Europe's privacy laws are far more consumer protective than our current scheme in the United States.

> *"It is our role as advisors to the media and entertainment industry to help craft and further corporate policies, industry self-regulation, and best practices (along with governmental regulation) in a manner that protects the interests of both consumers and industry, and fosters (rather than fetters) commerce."*

Another hot topic this year is mobile media: applications for Apple, Android, and Blackberry mobile smartphones permit easy access to content and communications, and provide new and interesting ways to use our mobile devices. Dan Schnapp's article *App-enectomy: Removing the Mystery from the App Ecosystem* explains the many issues that a company needs to address before launching an app. Not surprisingly, he identifies privacy as a key concern. Tanya Forsheit gets more specific with regard to privacy issues arising out of location-based functionality—a feature popular with many new app services.

2011 appears to be the year with very real potential for a federal consumer data privacy and data security scheme. The FTC is also expected to make recommendations regarding potential changes to the Children's Online Privacy Protection Act ("COPPA"), and only last month it settled a COPPA case against a social game publisher for a whopping $3 million—almost double the aggregate of fiscal remedies in all fifteen FTC COPPA enforcement actions that preceded it. It is clear that both this administration's FTC (as well as the administration itself and many members of Congress) are seeking to hold industry much more accountable for what they perceive as inadequate collection, use, sharing, and maintenance of consumer data. Stakeholders need to get involved in the legislative and regulatory process, and should have a senior level point person (such as a Chief Privacy Officer) to assist the company in keeping up with (and complying with) the changing law and the industry best practices. Beware that in the absence of comprehensive consumer data privacy legislation, the plaintiffs' class action bar stands ready to bring claims against companies failing to meet current obligations and who attempt to change industry practices.

Companies need to be certain that they are complying with the privacy and data security promises they make, and also make efforts to use disclosures that are consumer friendly. Regular audits of a company's privacy and data security practices and policies by privacy lawyers and information technology professionals is essential. Furthermore, it is recommended that companies adopt and follow industry self-regulatory principles and best practices, such as the new online behavioral advertising "iconic notice" program and October 2010's self-regulatory principles for online behavioral advertising adopted by more than a half-dozen of the leading advertising and business trade organiza tions that joined together as the Digital Advertising Alliance ("DAA"), principles which put the notice and opt-out on the ad (instead of within a privacy policy a consumer viewing the ad would arguably never see). For more information, see www.aboutads.info. For good resource on privacy and data security law, see the web site of the International Association of Privacy Professionals (www.privacyassociation.org), and my law firm's privacy resource center at http://privacylaw.wildman.com/index.cfm?fa=resourcecenter.home.

Finally, the FTC can be expected to ramp up repercussions for sellers that fail to ensure the principles set forth in the *Guides Concerning the Use of Endorsements and Testimonial in Advertising* are followed with respect to their online and social media promotional activities, including efforts to engage consumers, celebrities, bloggers and others with their brand. The recent $250,000 settlement with the FTC (discussed in Taylor's article) represents the first direct monetary repercussions for online marketers who fail to take reasonable steps making sure that those they provide consider-

ation to promote their products via social media clearly disclose the nature of the relationship and value received. Just as this edition of *Insights* was going to press on May 31, the FTC announced its first settlement involving a consumer charged with making misrepresentations in a product or service testimonial. Hollywood talent acting as spokespersons should take note. It would also not be surprising to see deceptive social media promotional practices spawn consumer class actions and/or state Attorney General actions, or claims by competitors (Kim Kardashian's allegedly paid tweets for one diet have already spawned a lawsuit against that diet promoter by a competitor diet service) as the issue becomes more newsworthy. Accordingly, companies need to take proactive steps to establish policies consistent with the FTC's guides—and to undertake reasonable monitoring and enforcement programs.

As convergence has given media and entertainment companies new tools for interacting with consumers and for distributing content, it has created issues like privacy and data security that must be dealt with by the lawyers that advise these companies. It is our role as advisors to the media and entertainment industry to help craft and further corporate policies, industry self-regulation, and best practices (along with governmental regulation) in a manner that protects the interests of both consumers and industry, and fosters (rather than fetters) commerce. The contributors to this issue provide valuable information and insights to assist you in this regard with respect to some of the biggest challenges facing our industry arising out of new media.

Enjoy.

GUEST EDITOR PROFILE

ALAN **FRIEL**

Alan Friel is a partner in the Intellectual Property Department of Wildman Harrold. He is a thought leader regarding convergence legal issues—the property, liability and regulatory implications at the evolving intersections between media, marketing, technology, distribution, commerce, privacy and communication brought about by the ongoing digital revolution.

A sought-after speaker and counselor regarding practical application of substantive legal issues, Mr. Friel is most proud of his long affiliation as an Assistant Professor in a multidisciplinary project at the Graduate School of TV, Film and Digital Media at UCLA where he helps groom the next generation of new media lawyers, executives and creatives. Mr. Friel has been contributing to the development of the legal and business paradigms of cyberspace since the days of CD-Rom and bulletin board services. He negotiated the first experimental Internet production agreements with traditional Hollywood talent unions—SAG, DGA and WGA—in the 1990s.

Mr. Friel continues to be on the cutting edge of emerging media, crafting alliances between TV pro-ducers and distributors and online services and between big brands and social game publishers and "app" developers, as examples. From major acquisitions to specific campaigns and basic online or mobile presence, Mr. Friel brings the experience and foresight necessary to help companies and entrepreneurs navigate the compelling, but complex, opportunities disruptive technology creates. His clients include both established and emerging companies. Mr Friel is AV® Preeminent™ 5.0 out of 5 Peer Review Rated by Martindale-Hubbell.

Contact: Friel@Wildman.com

COPYRIGHT AND FREE SPEECH IN THE AGE OF DIGITAL PIRACY

By Michael D. Fricklas

The relationship between copyright law and the First Amendment will define the future of artistic expression in the digital age as it has in every age since the advent of the printing press. Each of these pillars depends in large part on the other.

Indeed, Viacom, like many in the media business, depends on these pillars for the advancement of its interests. We own a movie studio and cable networks and have previously owned CBS and Simon & Schuster as well as radio stations across the country. In these roles, we have created valuable copyrighted works and have defended the rights of moviemakers, television journalists and authors around the world to be free of government interference, and have published books and distributed motion pictures that expose wrongdoing and highlight injustice. At core, however, what has made these actions possible are the protections provided for artists, investors and the public by copyright law.

Yet increasingly these rights are at risk. Creative industries are under assault from piracy, counterfeiting and digital theft. A careful study showed that the movie business alone loses more than $6 billion a year from piracy—and these figures do not include losses to countless other copyright-dependent industries or even account for the effect of illegal streaming services on movies' box-office performance.

But the risk to copyright is more than just financial.

There is a growing fringe that doesn't see copyright infringement as a problem. Its members make the argument that enforcing copyrights suppresses free speech; that it prevents ideas from being heard; and that those who would make a business practice out of violating copyright protection are standing up for openness, transparency and free expression. In a recent effort to enact legislation to combat online criminal behavior, these groups went so far as to claim that any governmental action would amount to "internet censorship."

These extreme views are distorted, dangerous and wrong. They represent a misguided interpretation of copyright law and a simplistic view of freedom of expression. If successful, they would result in a media environment that would punish artists and those that support them—while benefiting those who would steal their work for personal profit. What's worse, their views would actually contribute to less—not more—free expression.

From a legal perspective, copyright and free speech appear to be in tension.

On the one hand, the First Amendment of our Constitution offers strong and absolute language: namely "Congress shall make no law... abridging the freedom of speech..."

On the other hand, Article I, Section 8 of the Constitution authorizes Congress "To promote the Progress of Science and Useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries"—in short, the legal right to control writings and the practice of inventions.

Because these concepts were new, this is the only enumerated power of Congress that included an explanation. And the first Copyright law was adopted in 1790—a year *before* the First Amendment was approved by Congress.

None of this is accidental. As Justice O'Connor, writing in Harper & Row Publishers v. National Enterprises, commented on Article I, Section 8:

"[This] limited grant is a means by which an important public purpose may be achieved. It is intended to motivate the creative activity of authors and inventors by the provision of a special reward, and to allow the public access to the products of their genius after the limited period of exclusive control has expired."

At Viacom, we rely on fair use every day. Our television shows and movies use cultural references and make transformative uses of other people's works in exactly the way Congress intended. We have defended our rights in many important cases—resulting in decisions which benefit each of us as speakers.

Free speech is not the same thing as unlimited speech.

Exceptions to unlimited speech—that are in pursuit of the public purpose—are not unusual.

You cannot, for example, shout "fire" in a crowded theater. There is the law of libel, the law of securities regulation, laws prohibiting false claims about products, and laws preventing making untested claims about medicines. There is the law of conspiracy and there are laws protecting your privacy. There is, after all, a significant difference between message-based restrictions on political speech, which are protected to a very high degree, and other sorts of communications which receive little or no protection under the law.

Copyright protection is, of course, not absolute either. It is bounded by the concept of fair use. And even more fundamentally, it is bounded by not protecting ideas *at all*.

Again in the words of Justice O'Connor, this concept "strike[s] a definitional balance between the First Amendment and the Copyright Act by permitting free communication of facts while still protecting an author's expression."

A frequent academic concern is that intellectual property might infringe upon the commons: creating property around what already exists in the public domain and—in this way—stifling innovation and depriving the public of benefits what we all own collectively.

For example, one recent popular book on copyright complains that "intellectual property law" allows propertization of elements of the human genome. However, a book on the genome imposes no limits to the number of people who can write about the genome—only a limit on directly copying someone else's efforts to do so.

It is copyright that finances the referenced book that talks about the genome, from which the public benefits. The irony, of course, is that if one followed the author's advice to its logical conclusion—and weakened copyright protections—it would undermine the very economic incentives that would create the book to teach us about this basic science in the first place.

Of course, not all speech requires a financial incentive. Much of the artistic content that we enjoy is created out of a desire to participate in public debate, to contribute to the arts, or because it is supported a different way, such as through an academic salary.

But just as open source software and proprietary software coexist, so, too must public speech and privately-financed speech. Also, particularly in the movie and television business, the need for large amounts of capital and the coordinated, full-time effort of very large teams mean that volunteerism isn't going to provide the necessary support. In this digital age, it has become more and more difficult to protect copyrights, particularly as new technological advances make it easier to steal protected material. It is also easy for some people to look the other way, particularly when infringement of other people's copyrights makes them lots of money. They claim that limiting copyright infringement is the same thing as preventing the general public from learning about their government. A lot of these people claim that imposing any level of responsibility, even not to engage in willfully blind behavior, infringes on their rights, or the rights of the people who use their services. These people fail to distinguish between the right to free speech, and the right to use the speech of someone else for free.

There is a lot that can be done, and must be done, about infringement, and these steps not only don't harm free speech—they are fundamental to free speech. That's why standing up for this most basic of artistic rights is truly more important now than ever.

AUTHOR PROFILE

MICHAEL D. **FRICKLAS**

Michael D. Fricklas has served as Executive Vice President, General Counsel, and Secretary of Viacom Inc. since January 2006. Mr. Fricklas is responsible for the legal affairs of Viacom and its subsidiaries, including management of Viacom's Law Department.

Previously, Mr. Fricklas served as General Counsel and Secretary of the former Viacom Inc. since October 1998. Mr. Fricklas joined the former Viacom as Vice President, Deputy General Counsel in 1993. During his tenure, Mr. Fricklas has played an integral role in guiding complex corporate transactions, in coordinating the company's legal and business affairs activities, and in upgrading Viacom's Law Department.

Before joining the former Viacom, Mr. Fricklas spent three years as Vice President, General Counsel and Secretary at Minorco (U.S.A.) Inc., which was responsible for Minorco's North American mining and agribusiness operations and investments. From 1987 to 1990, Mr. Fricklas was with Shearman & Sterling, where he specialized in corporate finance and mergers and acquisitions. Earlier, Mr. Fricklas was with Gray, Cary, Ware & Freidenrich, in Palo Alto, Calif.

Mr. Fricklas received a B.S.E.E. from the University of Colorado's College of Engineering and Applied Sciences in 1981 and a J.D., *magna cum laude,* from Boston University School of Law in 1984. Mr. Fricklas serves on the board of trustees of Jazz at Lincoln Center, President of the Association of General Counsel, Advisor of the World Policy Institute, and on the board of visitors of the Boston University School of Law. He is a member of the executive committee of the general counsel committee of the business law section of the American Bar Association; the general counsel committee of the National Center for State Courts and the Association of General Counsel.

TOUGHER COPYRIGHT LAWS WON'T SOLVE BIG MEDIA'S INTERNET PROBLEM, BUT THEY WILL STIFLE INNOVATION

By Robert Tercek

Entertainment studios don't have a legal problem on the Internet. They have a business model problem. Calls for ever-more government regulation to enforce intellectual property rights online are doomed to failure.

Case in point: On May 24, 2011, at an invitation-only gathering in Paris prior to the G8 summit, French President Nicholas Sarkozy boldly proclaimed his intention to expand government regulation of the Internet. The announcement brought cheers from media executives and jeers of derision from technology leaders, including Google Chairman Eric Schmidt and Facebook founder Mark Zuckerberg.

But Sarkozy's carefully stage-managed pronouncement was undermined by two significant developments.

First, new research published by Sandvine, a Canadian company that analyzes traffic on broadband networks, illuminates major changes in content consumption in the US, Latin America and Europe. The consumption of paid legal content is growing swiftly, outpacing illegal file sharing for the first time. In the USA, online video provider Netflix now accounts for 30% of all bandwidth consumed at peak times in the US. However in Europe, where Netflix is not yet available, the largest percentage of bandwidth is consumed by BitTorrent, the peer to peer software platform that is notorious for enabling illegal filesharing.

The data is unambiguous. In markets where movie and TV studios make it easy and legal for consumers to access their wares, the growth of illegal file-sharing diminishes. Immediately. Conversely, where legal access to copyrighted content is not available, file-sharing comprises the single biggest chunk of traffic.

This data supports the common-sense observation that most people would prefer not to steal. If they can enjoy entertainment on their terms at a reasonable price, they are prepared to pay for it rather than contend with the risks of dubious grey-market wares.

If media companies want to stop intellectual property theft, they must make their wares available on terms that consumers find reasonable. That's a business model solution.

The second development is the news that the software developed by the French government to track illegal file-sharing is riddled with major security flaws. Hackers were able to penetrate the system with ease to extract data, including private user information. Even worse, TMG, the firm hired by the French HADOPI agency to collect piracy data, failed to take precautions to secure the servers, leaving them vulnerable to hackers who could hijack the equipment to install their own malicious code. The tech blog Ars Technica reports that the system developed by TMG is so deeply flawed that the government was obliged to suspend its much-ballyhooed "three strikes" policy to track pirates.

This embarrassing failure underscores the immense difficulty of implementing a rigid regulatory regimen that can keep pace with the rapid evolution of a new medium. The Internet is designed to route around roadblocks, and regulatory hurdles are no exception. The French government inadvertently revealed the limitations of a bureaucratic approach to enforcing copyright law. The software developed by the French government failed so comprehensively that Sarkozy himself had to back down, dismissing it as a "temporary solution".

These two developments undermined Sarkozy's message. The solution to intellectual property theft isn't a tighter regulatory grip; the solution is to embrace the economics of the web.

Analysts are beginning to arrive at the conclusion that rigid IP laws are a problem, not a solution. In the UK, professor David Hargreaves delivered a report on intellectual policy in the digital age at the request of Prime Minister David Cameron. Professor Hargreaves concludes that existing policies are too restrictive and hobble innovation. Moreover, Hargreaves criticizes lazy legislators who develop policy by relying upon "the persuasive powers of celebrities and creative companies" rather than factual evidence. The result is flawed policy that serves rights holders at the expense of consumers and other participants in the evolving media ecosystem. As a remedy, Hargreaves proposes greater flexibility in IP laws with more exceptions to enable innovative uses of copyrighted material.

Too bad Hargreaves' message was ignored by US legislators who propose ever-tighter restrictions on consumer behavior, such as the PROTECT IP Act introduced in the Senate. This law would block access to international file-sharing sites that provide access to a mixture of legal and pirated content. This overbroad law would put the US on par with the Chinese government and Middle Eastern despots who seek to limit their citizens' access to information and free expression.

We're witnessing a clash between two dramatically different business models. The battle over IP laws is just a sideshow.

The Internet challenge to traditional content industries is all about control. Consumers want to exert more control over their personal media, but the media companies want to exert more control over their consumers.

For decades, the audience had to play by the rules set by the publisher or distributor. If we wanted to watch a particular show, millions of us had to rearrange our schedules to tune in at 8:00. A hit song? To hear it, we had to buy it on an album bundled with 11 other tracks that we didn't want. Our favorite cable channel? To see it, we were obliged to subscribe to a bundle of channels that we didn't want and would never watch.

No surprise that consumers have adopted digital technology with gusto. The unbundling of mass media is well underway and it cannot be undone.

Digital media give the audience unprecedented ability to manage their media consumption on their own terms. The consumer audience has demonstrated that they don't want their content sold in bundles, albums, or packages. Instead, they rip, burn, mix and create their own playlists of singles and shows packaged to individual preference.

> "In markets where movie and TV studios make it easy and legal for consumers to access their wares, the growth of illegal file-sharing diminishes immediately. Conversely, where legal access to copyrighted content is not available, file-sharing comprises the single biggest chunk of traffic."

For today's audiences, WWW doesn't mean the World Wide Web. It stands for "Whatever, whenever, wherever".

Instead of celebrating the customer's newfound enthusiasm for their wares, old media companies are trying to turn back the clock. They're working overtime to resurrect the obsolescent business model from the previous century and transplant it onto the Internet, and they're enlisting government officials to enact ill-conceived and unenforceable regulation as an extra coercive measure.

However, this strategy hasn't worked very well. The problem is that the old media giants are attempting to impose artificial scarcity on a new platform that is optimized to deliver exactly the opposite experience: limitless abundance.

The result is a ghastly spectacle of marketing incompetence. In order to reinforce the illusion of scarcity, media giants have placed every conceivable obstacle in front of their customers. There are plenty of examples. For instance, iTunes digital movie rentals arbitrarily expire in 30 days if they have not been viewed. They disappear 24 hours after you start watching them, whether or not they have been viewed to completion. If you are interrupted after you've started watching, too bad. Some online video services cannot offer the most popular TV shows at any price because studios refuse to license them. On most cell phones, the only way to access popular TV shows is via the carrier's cumbersome interface. On cable television's VOD service, popular shows are only available for a short period of time. On the iPad, magazine apps are absurdly overpriced: a digital copy should not be the same as the printed issue on the newsstand. The price of digital books is kept deliberately high by publishers in order to stave off the inevitable erosion of prices for print editions. The publishers seem determined to make it more difficult to consume their products.

These are not smart business decisions. They are obstacles designed to coerce customers into playing by big media's rules.

Ultimately, these measures will prove self-defeating. The second century of electronic media is less about "content is king" and more about "the consumer rules."

Defenders of old media claim that they need extra firepower to fight pirates and copyright infringement on digital platforms. Paradoxically, the onerous rules imposed by media companies are the biggest cause of piracy.

When consumers are given the ability to enjoy content legally in the format of their choice, they opt for it. But when the goods are encumbered with arbitrary rules that limit the ways that customers can use them, the audience responds quite naturally like the Internet: they route around these damaged goods and seek out a grey market alternative.

Economist Umair Haque of the Havas Media Lab explains that consumers perceive *less value* in content that is encumbered with digital rights software or other restrictions than an unrestricted version of the same content. Nevertheless, media companies insist on charging a premium as if the restrictions somehow enhance the value of the content.

They do not. They make the content harder to consume. And customers understand this instinctively.

Consumers have voted with their remote controls and their dollars. They are migrating en masse to the services that offer maximum flexibility and choice. That's the real reason why Netflix has grown so dominant. No other online content service caters to the customer as much as Netflix. With Netflix, you can watch any program on any device, stop it in mid-stream, walk into another room and resume viewing on an entirely different device at a later time.

The vanity of many a movie studio executive was bruised by recent reports about Netflix usage. Contrary to industry insider expectations, consumers did not care very much that Netflix lacks the big hits or the most current releases. It turns out that subscribers are quite content to substitute one film for another, much to Hollywood's chagrin. A huge percentage of what's viewed on Netflix consists of archive films and old episodes. What the consumers crave is control.

Consumers naturally move to those services that give them greater control over when, where and how they consume entertainment. This trend is unstoppable.

Netflix really shouldn't exist at all. If the media companies and the cable system operators were innovating instead of wasting their efforts fighting the future, they would have invented unlimited on-demand "instant viewing."

Since the advent of commercial content on the Internet in 1996, the large entertainment conglomerates have adopted an antagonistic approach to new media. Instead of embracing the new medium and developing content and services that are appropriate to the medium, they have invested time and treasure into lobbying efforts to preserve a crumbling business model and lawsuits to hobble the migration to digital platforms.

This approach hasn't proven very successful. Media companies have very little success to show for their efforts. Typically, they buy in too late. News Corporation's humiliating failure to manage MySpace is just the latest in a long series of abortive efforts to buy a seat at the table long after the game has moved elsewhere.

Meanwhile, billions in new wealth has been generated by made-for-the-medium startup ventures that were unencumbered by a legacy business. The Internet has proven to be an economic powerhouse as well as the most fertile terrain for innovation in communications and entertainment.

According to a report published this week by McKinsey Global Institute, the Internet comprises 3.4% of the GDP in 13 countries, significantly more than heavily subsidized sectors like utilities and agriculture. Even more striking, the Internet accounts for a whopping 21% of economic growth. The McKinsey study evaluated the Internet in 13 countries, including the G8 plus China, Brazil, India, South Korea and Sweden. At a time when the reliable revenue drivers for major media have ceased growing (cable television) or are in free fall (sales of recorded media on CD and DVD), this report gives us an occasion to consider how the Internet is re-shaping the media landscape for a dynamic new century.

In the midst of a feeble economic recovery, it defies logic that the government would support big media's effort to stifle innovation in the one field that has generated billions in new wealth, thousands of new companies, and millions of high quality white-collar jobs.

The solution to a lagging economy is not to cripple a dynamic growth industry with constraints that favor aging giants who ceased innovating decades ago; the solution is to promote investment in broadband network upgrades to keep the US competitive with leading Asian and European nations, where consumers enjoy residential broadband at speeds ten times faster than the US for half the price.

AUTHOR PROFILE

ROBERT **TERCEK**

Robert Tercek (www.roberttercek.com) has launched media ventures internationally on every digital platform, including satellite television, game consoles, broadband Internet, interactive television and mobile networks. Prior to founding the General Creativity strategic advisory firm, he served as President of Digital Media at OWN: The Oprah Winfrey Network. Previously he served in senior management at Sony Pictures, PacketVideo and MTV. He has served as an advisor to major media and technology companies as well as several startups, including BrightCove, M:Metrics, Visual DNA, and Scoreloop AG.

Contact: email@Tercek.com

LOCATION INFORMATION: INCREASING CONCERNS

By Tanya L. Forsheit & Nicole Friess

Recently, location information has become a hot topic of discussion. Businesses are increasingly collecting, using, and storing location information. These information practices have raised concerns regarding the privacy rights and personal safety of consumers, and lawmakers are considering the adoption of specific laws governing location data. So why is location information such a big deal?

LOCATION INFORMATION

Service providers maintain databases of the locations of certain mobile cell towers and Wi-Fi access points. They use this data to calculate an approximate location of a user's device by comparing the Wi-Fi access points and cell towers that the device can detect to the location database, which contains correlations of known Wi-Fi access points and cell towers to observed latitudes and longitudes. In many cases, a mobile device's location can be determined within 100 feet.

LOCATION-BASED SOCIAL NETWORKS AND SERVICES

Location-based services are accessible using a mobile device and utilize the device's geographical position. These services offer many benefits to users, making it easy to find nearby stores, get directions to desired destinations, retrieve up-to-date weather forecasts, play location-based games, and view promotions or receive coupons from businesses in the user's vicinity.

Location-based social network platforms such as Foursquare, Gowalla, and Facebook Places allow users to check-in at various venues using a smartphone app or SMS. Users can share their whereabouts with their social media networks by posting the users' locations to their Facebook, Twitter, or other accounts. Merchants and brands leverage these platforms by utilizing a wide set of tools to obtain, engage, and retain customers and audiences. Increasingly, app developers are using these location-based social networks to create games, challenges, city guides and dating services. While some apps require users to take affirmative steps to check-in to venues and share their location, new apps are available that automatically check users in to a location when they are within a short distance of that location.

THE PRIVACY PROBLEM

The flurry of activity surrounding location information was spurred when researchers revealed that some mobile devices were storing up to a year's worth of location data on peoples' devices in an apparently insecure manner. Privacy advocates, members of Congress, and consumers share a number of concerns regarding the privacy implications of the collection and use of location information. The following concerns have become the focus of the debate:

User Comprehension—One central concern is that consumers do not fully understand how location information is collected, how service providers use that information, and with whom they share it. Location information can be particularly sensitive as it pinpoints users' whereabouts and, if tracked over an extended period of time, reveals much more than just a snapshot in time. According to the Center for Democracy and Technology, "location information reveals physical destinations such as medical clinics or government services buildings." One unintended consequence of location data tracking might be third parties' new ability to draw conclusions based on location data. For example, location information may allow a third party to infer that a person suffers from a specific health condition or other sensitive information—information that is often protected by laws that limit access to such data.

Users can understand how their location data is collected and used if they can review a privacy policy explaining information practices. However, a survey by the Future of Privacy Forum revealed that 22 out of the top 30 paid mobile apps lacked a basic privacy policy. Similarly, the Wall Street Journal reviewed the top 101 iPhone or Android apps and found that 45 of them did not provide privacy policies on their websites or inside the apps at the time of testing.

User Control—Another widely-shared concern is that location data is increasingly collected and used by service providers without users' consent. Data about users' locations and historical movements is owned and controlled by the network operators, including service and content providers. On May 19, 2011, the Senate Commerce Subcommittee on Consumer Protection, Product Safety, and Insurance held a hearing entitled "Consumer Privacy and Protection in the Mobile Marketplace," to discuss consumer privacy concerns and explore the possible role of the federal government in protecting mobile device users. Senator Jay Rockefeller (D-WV) voiced his concern that, as mobile devices become more powerful, more personal information is concentrated in one place, possibly resulting in unintended consequences for users. Consumers share this concern—a survey commissioned by the privacy certification company TRUSTe found that 98 percent of consumers express a strong desire for better controls over how their personal information is collected and used by mobile devices and apps.

Who Is/Should be Responsible?—Despite recent reports that the Apple iPhone, Google Android phones, and other mobile devices are collecting, storing, and tracking user location data without the user's consent, a Google representative testified before Congress that "location sharing on Android devices is strictly opt-in for our users, with clear notice and control." Similarly, a representative from Apple testified that "Apple does not track users' locations. Apple has never done so and has no plans to do so."

While service providers may provide users with notice and control over their location data, privacy issues get complicated when third-party apps are involved. Apple testified before Congress that it requires app developers to agree in writing to obtain users' opt-in consent before using location data. Apple, however, does not monitor applications after they are made available to consumers. To date, Apple has not removed any apps from its store due to location-based violations. Additionally, Google testified that it "does not and cannot control the behavior of third-party applications, or how they handle location information and other user information that the third-party application obtains from the device."

LEGAL FRAMEWORK IN THE U.S.

The FTC has "a number" of open investigations targeting mobile-phone privacy practices, according to David Vladeck, director of the FTC's Bureau of Consumer Protection. The agency is increasingly bringing enforcement actions against companies that violate their own privacy policies. However, as noted above, many mobile apps lack even a basic privacy policy, which gives the FTC little authority to take action, according to Vladeck. With no law specifically governing location data practices, smartphone apps are "totally unregulated" in terms of privacy protections, according to Senator Rockefeller.

However, there is a growing buzz of activity in Congress aimed at protecting consumer privacy online and in the mobile arena. Notably, Senators John Kerry (D-MA) and John McCain (R-AZ) introduced the "Consumer Privacy Bill of Rights Act of 2011" that proposes rules based on fair information practice principles applicable to mobile devices. Senator Rockefeller recently introduced the "Do Not Track Online Act of 2011," which would give the Federal Trade Commission authority to require app providers to implement privacy protections.

RECOMMENDATIONS

Location-based services and check-in apps are not without their benefits, but the current lack of transparency regarding how location information is collected and used has raised numerous concerns. Service providers and app developers can adopt technical approaches to protect consumer privacy using privacy-enhancing technologies, such as providing users with a switch to turn off location tracking and implementing data anonymization techniques. Additionally, service providers and app developers are encouraged to use "best practices," such as requiring users to opt-in to the use of their location data, creating clear and concise privacy policies, and minimizing the data they collect. Whether or not legislation controlling the collection and use of location information is codified in the near future, those handling location data should assess and attempt to address the privacy concerns of consumers and regulators up front to avoid consumer backlash and regulatory investigation down the line.

AUTHOR PROFILE

TANYA L. **FORSHEIT**

Tanya L. Forsheit is one of the Founding Partners of InfoLawGroup LLP. Tanya founded InfoLawGroup in 2009 after 12 years as a litigator and privacy/data security counselor at Proskauer where, most recently, she was Co-Chair of the firm's Privacy and Data Security practice group. Certified as an information privacy professional by the International Association of Privacy Professionals, Tanya works with clients to address legal requirements and best practices for protection of customer and employee information. In 2009, Tanya was named one of the Los Angeles Daily Journalís Top 100 women litigators in California. Tanya is President-Elect of the Women Lawyers Association of Los Angeles and is a Trustee of the Los Angeles County Bar Association. She graduated from the University of Pennsylvania Law School, and received her AB in Political Science and English from Duke University, cum laude.

Contact: Tforsheit@infolawgroup.com

AUTHOR PROFILE

NICOLE **FRIESS**

Nicole Friess is an associate at InfoLaw Group LLP. Before joining the Information Law Group, Nicole worked in the Samuelson-Glushko Technology Law and Policy Clinic at the University of Colorado Law School. As a student attorney, Nicole helped write amicus briefs involving the Electronic Communications Privacy Act and constitutional privacy issues to the Ninth Circuit Court of Appeals, the Eleventh Circuit Court of Appeals, and the Supreme Court of the United States. Nicole received her law degree from the University of Colorado Law School in 2010. During law school, Nicole was awarded a fellowship from the Women's Law Caucus and a fellowship from the Public Interest Law Student's Association. She participated in the Colorado Law Public Service Pledge and volunteered over 100 hours to law-related public service work. After her second year of law school, Nicole clerked at the Texas Civil Rights Project where she worked to promote racial, social, and economic justice through litigation involving privacy, voting rights, police misconduct, sex discrimination, employment bias, disability rights, and traditional civil liberties.

Contact: nfreiss@infolawgroup.com

EUROPE IMPLEMENTS NEW "COOKIE LAW": MAY 25, 2011

By Nick Graham

Europe's new rules on the use of website cookies and similar technologies for storing information on a user's computer or mobile device come into force on May 25, 2011. These rules are contained in the changes to the e-Privacy Directive (2002/58/EC), which also introduces a new data breach notification requirement for telecoms companies and ISPs. The new rules impact all websites and services organized from or directed at the European Union, and so may catch US and international businesses operating in Europe.

NEW LAW ON COOKIES

A cookie is a small file that can be downloaded to a PC or mobile device when the user accesses certain websites. A cookie allows the website to "recognize" the user's device. Cookies are used to enable websites to deliver a more customized and user-friendly experience. They are also used to gather data about users, which raises the issue of privacy.

The current EU rules say that a person must not use an electronic communications network to store information, or gain access to information stored, in the terminal equipment of the subscriber or user unless the subscriber or user is provided with clear and comprehensive information about the way in which the cookies (or other technology) are used.

Usually, this explanatory information is contained in the website privacy policy, which also explains how the subscriber or user can delete or refuse cookies. The current rule applies to all storage of or access to "information" (not merely personal data).

The new rules are contained in Article 5(3) of the e-Privacy Directive, which will be implemented in the UK by an amended Regulation 6 of the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR). The new rules add an additional requirement in that you must obtain the consent of the relevant subscriber or user in order to store, or gain access to, information in the terminal equipment of the subscriber or user.

There is a limited exemption from the new consent rule in relation to the technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network or as strictly necessary in order for the provider of an information society service (i.e. an online/e-commerce service) explicitly requested by the subscriber or user to provide the service. However, this will not exempt many of the cookies commonly used by website operators and adservers.

pg. 20 to 27
ONLINE BEHAVIORAL ADVERTISING LITIGATION AND PROPOSED LEGISLATION: LESSONS FOR ONLINE PUBLISHERS AND ADVERTISERS

pg. 28 to 31
RECENT FTC ENFORCEMENT ACTIONS INVOLVING ENDORSEMENTS, PRIVACY AND DATA SECURITY

pg. 32 to 36
APP-ENDECTOMY: REMOVING THE MYSTERY FROM THE APP ECOSYSTEM

pg. 37 to 39
SOCIAL NETWORKING: WHY CAN'T WE BE FRIENDS?

NEW LEGAL GUIDANCE PUBLISHED IN THE UK

One of the key issues with the new rules on cookies is how and whether website operators can collect individual consents for the use of cookies without impacting the user experience. For example, introducing a "pop-up box" to ask for consent prior to allowing the user to view a website could have a substantially detrimental impact on user experience. However, the Article 29 Working Party (the independent European advisory body on data protection) published guidance last year saying that browser settings (potentially a much more pragmatic way to obtain user consent) are unlikely to deliver consent, except in very limited circumstances. This is undoubtedly the correct legal analysis based on the Data Protection Directive (94/6/EC), which requires consent to be a freely given, specific and informed indication of the individual's wishes. Nevertheless, there has been much debate in the past six months as to how website operators can obtain user consent in both a pragmatic and a legally compliant manner.

Last week, the UK data protection regulator (the Information Commissioner's Office (ICO)) published guidance on the new rules on cookies and, in particular, how to obtain consent in a pragmatic way. Unfortunately (but perhaps not surprisingly) the ICO takes the view that you cannot rely on browser settings to deliver consent for the use of cookies. This may change in the future as there are various industry initiatives to work with the browser manufacturers to embed privacy preferences within individual browsers. Suppose, for example, that a user is asked to state their privacy preferences (and whether they wish to allow cookies) when they first use the browser and, perhaps, at regular intervals thereafter. We believe this would create the required consent without impacting user experience. In the absence of such a solution, the ICO guidance discusses use of pop-ups, terms and conditions and other practical steps that can be taken to obtain consent. The guidance also highlights the particular difficulties where websites allow third parties to set cookies on a user's device. This can be a particularly challenging area for websites that display content from third parties, and impacts directly on online behavioural advertising and advertising networks.

IMMEDIATE ACTION REQUIRED

In practice, the new rules on cookies will apply to all website operators who use cookies or similar technologies. The exceptions are very narrow. While the new rules can be implemented by websites to the extent that users log in/sign on to receive a service, the issue is much more challenging where websites use cookies in relation to subscribers or users who simply visit the website in the normal way.

The ICO advises you to take the following steps now:

1. Check what type of cookies and other similar technologies you use and how often you use them.
2. Assess how intrusive your use of cookies is.
3. Decide what solution to obtain consent will be best in your circumstances.

It is important for businesses to address the above questions. If the ICO receives a complaint about a website, the ICO will expect an organisation's response to set out how is has considered the above points and that it has a realistic plan to achieve compliance. The ICO guidance is quite clear: doing nothing is not an option.

The ICO will be issuing separate guidance on how it intends to enforce the new rules.

DATA BREACH NOTIFICATION

The update to the e-Privacy Directive (2002/58/EC) also introduces a new data breach notification requirement. This applies to the providers of publicly available electronic communication services (i.e. telecoms companies and ISPs). In the event of a "personal data breach" the communications service provider must notify the relevant data protection authority "without undue delay"' The provider is also required to notify the relevant subscribers or individuals where the breach is likely to adversely affect the personal data or privacy of subscribers or individuals.

The new rules also require providers to maintain an inventory of personal data breaches (i.e. a data breach log) comprising the facts surrounding each breach, its effects and the remedial action taken. The national authorities in each EU member state can also audit individual providers as to whether or not they have complied with their obligations.

THE NEW RULES PRESENT A CHALLENGE

The new rules on cookies present a challenge for all businesses that operate websites, serve or use banner advertisements, run advertising networks or provide online/e-commerce services in or directed at Europe. How do they obtain consent without damaging user experience? The ICO guidance is a helpful summary of the new rules and provides a view on some of the practical and technical steps that businesses can use to obtain consent for the use of cookies. It is now clear that you cannot simply ignore the new rules. Positive steps must be taken to ensure compliance. The practical steps required will depend on the way in which your website operates and the nature of services/information provided.

INTERNATIONAL AND GLOBAL BUSINESS

The new rules also present challenges for US, international and global businesses. Implementation of these rules will be undertaken in each of the 27 member states of the European Union so it is quite conceivable that the detailed requirements will vary from one member state to another. In addition, the EU "consent-based" solution is the reverse of the industry-led approach in the United States, where users are provided with information and an opportunity to opt out of the use of cookies. The challenge for US and international business, therefore, is whether to implement a European-specific solution for European users only or apply the "European model" to other jurisdictions in the interests of consistency.

AUTHOR PROFILE

NICK GRAHAM

Nick Graham is a partner at SNR Denton (www.snrdenton.com) specializing in technology transactions, IT and business process outsourcing, acting for both customers and suppliers in both public and private sectors including business process re-engineering and off-shoring. Mr. Graham also specializes in IT law, e-commerce, is an expert in data protection and freedom of information and is head of the firm's Data Protection and Privacy Group, and Mr. Graham has advised on innovative and complex data protection solutions including for CRM strategy and international data transfers.

Contact: Nick.Graham@snrdenton.com

ONLINE BEHAVIORAL ADVERTISING LITIGATION AND PROPOSED LEGISLATION:

LESSONS FOR ONLINE PUBLISHERS AND ADVERTISERS

By Dominique Shelton & Alan Friel

Online behavioral advertising ("OBA"), which involves tracking of users to build user profiles and serve them contextually relevant ads, is reportedly more than twice as effective in converting viewers to buyers than traditional online ads and twice as effective in securing revenue per ad. Given that in 2010 online ad spending for the first time exceeded that of print advertising, the ability of digital media to utilize OBA to more effectively target specific consumers—and consumers' flight from print to digital publications—seem to have contributed to this growth. While this may seem to be good news for digital publishers and advertisers, 2010 and 2011 have been marked by the rise of regulatory, legislative and litigation activity surrounding the question of the appropriateness of OBA and what level of notice and consent should be afforded consumers.

The Federal Trade Commission ("FTC") defines behavioral advertising as "the process of tracking consumers' activities online to target advertising." It often, but not always, includes a review of the searches consumers have conducted, the webpages visited, the purchases made, and the content viewed, all in order to deliver advertising tailored to an individual consumer's interests. While the FTC and self-regulatory groups have been discussing this issue for years, it appears that litigation and legislation concerning this issue will peak in 2011-12. Already, the FTC has closed the public comment period for a "Do Not Track" option to be added before targeted advertising can be served. As of March 2011, there were 449 comments. As more fully explained in this issue's article by Nick Graham, the European Union, which has greater levels of consumer privacy protection than the U.S., passed a new privacy directive that went into effect on May 25, 2011 that requires "explicit" consent before cookies and other tracking devices can be enabled on a consumer's computer. The call for a U.S. nationwide privacy protocol, achieving greater harmonization with more stringent international standards, has caught the interest of legislators in the United States; on March 16, 2011, the Obama administration called for a universal privacy bill, and specifically supported the FTC's "Do Not Track" proposals.

ENTER THE CLASS ACTION BAR

As legislators, regulatory agencies, consumer groups and industry debate the issues publicly, the plaintiffs' bar has seized the opportunity to step up class action activity based on a number of theories. A summary of some of the recent results obtained in 2011 provides insights into strategies and tactics that might be used by plaintiffs and defendants in the remaining 30-plus class actions that are currently pending in state and federal court across the country.

The ISP Cases

The first wave of federal class actions filed in February 2010 were focused on cable companies providing Internet services. On February 3, 2010, a putative class action was filed in the Northern District of Alabama Styled: Green v. Cable One (Case No. 1:10-cv-00259). Cable One, a division of the Washington Post, is an Internet Service Provider ("ISP") that provides online services.

In Green, the named plaintiff alleged that Cable One entered into a contract with the (now defunct) third-party advertising-server, NebuAd. Pursuant to the contract, Green alleged that Cable One "began installing 'spyware devices' on its broadband networks." Green also alleged that Cable One added "appliances" to its modems and that these "devices funneled all affected users' Internet communications—inbound and outbound in, their entirety—to ...NebuAd." Green further challenged Cable One's use of so-called "super persistent" tracking "cookies" that were not detectible through security and browser settings which allegedly permitted Cable One to use "deep packet inspection technologies" to serve ads. Green further contended that Cable One and NebuAd interrupted communications with websites to include targeted advertising "other than those authorized by the publishers of the web pages downloaded by users."

Green alleged four causes of action: (1) Invasion of Privacy by Intrusion Upon Seclusion; (2) Violations of the Electronic Communications Privacy Act ("ECPA" or Wiretap Act) (18 U.S.C. § 2510) for the deployment of the appliance and interception and use of personally identifiable information; (3) Violations of the Computer Fraud and Abuse Act ("CFAA") (18 U.S.C. § 1030) for intentionally accessing users' communications in a manner that caused damage; and (4) Trespass To Chattel by interfering with the operation of the users' computers.

Green filed a motion for class certification in August 2010. Shortly thereafter, Cable One requested to inspect his computer. Green refused, then voluntarily dismissed (with prejudice) three of his claims that depended upon allegations of harm, leaving only the ECPA remaining. On November 9, 2010, Green was deposed. He testified that he accessed his Cable One account exclusively from his home in Alabama. This admission proved fatal. Cable One's records revealed that Green's Internet subscription had been canceled one day before the NebuAd ad contract went into effect. Accordingly, Cable One filed a motion to dismiss on the ground that Green lacked Article III standing, and the Northern District of Alabama agreed. The case was dismissed on February 23, 2011.

The result in Cable One shows that no matter how inflammatory the privacy allegations may appear in the complaint, courts will look closely at the factual issues to determine whether the named plaintiffs can even pursue them. Green's refusal to permit review of his computer for purposes of determining harm under the CFAA proved costly—forcing premature (albeit voluntary) dismissal of that claim as well as others. The viability of the substantive claims, however, remain open questions.

On February 16, 2010, a class action lawsuit was filed against another ISP styled: Mortensen v. Bresnan Communications LLC, 1:10-cv-00013 (United States District Court, District of Montana). The Mortensen complaint was filed by the same law firm as the Green action and contained many of the same allegations. The Mortensen plaintiffs alleged that from early 2008 through June of 2008, Defendant Bresnan Communications ("Bresnan") diverted substantially all of their Internet communications to NebuAd. As was alleged in the Green case, the Mortensen Plaintiffs alleged that Bresnan modified its network to permit NebuAd to install its "appliance." The Mortensen Plaintiffs further alleged that NebuAd used the appliance to gather information to create profiles of Bresnan's customers to serve interest-based ads. The Mortensen plaintiffs further alleged that Bresnan shared revenue with NebuAd and profited from the invasions of privacy. The same four causes of action alleged in the Green case were alleged against Bresnan– i.e., (1) Invasion of Privacy by Intrusion Upon Seclusion; (2) Violations of the ECPA (18 U.S.C. § 2510); (3) Violations of the CFAA (18 U.S.C. § 1030); and (4) Trespass To Chattel.

On April 23, 2010, Bresnan filed a motion to dismiss. First, Bresnan argued that plaintiffs failed to state a claim under ECPA. To prevail on an ECPA claim, the plaintiffs must demonstrate that the defendants (1) intentionally (2) intercepted or endeavored to intercept (3) the contents (4) of an electronic communication (5) using a device. Bresnan argued that it did not use a device to intercept plaintiffs' communications—NebuAd did—so Bresnan "cannot be liable for [NebuAd's] interception or use of electronic communications." Bresnan also argued that its cooperation in installing NebuAd's appliance on its network did not create liability under the ECPA. The Eighth Circuit previously ruled that "acquiescence in [another]'s plans to [engage in interception] and [] passive knowledge [thereof] are insufficient" to assign liability to a defendant under the ECPA. Bresnan further argued that "[e]ven where someone instructs another to intercept, no ECPA claim lies because the ECPA does not have an 'aiding or abetting' component."

"The call for a U.S. nationwide privacy protocol, achieving greater harmonization with more stringent international standards, has caught the interest of legislators in the United States; on March 16, 2011, the Obama administration called for a universal privacy bill, and specifically supported the FTC's "Do Not Track" proposals."

In their Opposition to Bresnan's Motion to Dismiss, the Mortensen Plaintiffs countered that Bresnan's liability was not limited to "aiding and abetting":

"Inasmuch as Bresnan concedes that it installed the NebuAd device into its network, its interception was intentional. Deployment of the appliance required Bresnan, physically, to take its cables that carried all user Internet traffic, outbound and inbound, and plug them into the appliance."

Bresnan also argued that two exceptions to the ECPA applied to its conduct. First, the ECPA excludes activities that are "a necessary incident to the rendition of [the ISP's] service." In its Opposition, the Mortensen Plaintiffs blasted Bresnan's contention that monitoring of user activity was a "necessary" incident to providing Bresnan's Internet services. In its December 2010 Order, the Montana District Court ruled: "that NebuAd and Bresnan deployed the Appliance on Bresnan's network infrastructure" and Bresnan had 'configured' its network to 'funnel all User Internet through the Appliance' were sufficient to show violations of the ECPA and were not 'necessary' functions of an ISP.

Second, Bresnan argued that the ECPA exclusion of situations where "one of the parties to the communication has given prior consent to such interception" applied. Bresnan contended that it had obtained "consent" to intercept the plaintiffs' communications via three documents: (1) Bresnan Communications OnLine Privacy Notice; (2) Bresnan's On-Line Subscriber Agreement and (3) an email notice to users that the NebuAd test was taking place which also contained instructions for users to opt-out. The Bresnan documents asked users to: "[A]cknowledge[] and agree[] Bresnan [] and its agents shall have the right to monitor... postings and transmissions, including without limitation... web space content." Brensan further contended that these documents notified "subscribers that Bresnan's 'equipment automatically collects information on your use of the Service including information on... the programs and web sites you review or services you order, the time [] you... view [them, and] other information about your 'electronic browsing.'" In addition, the documents disclosed to users that "Bresnan [], its partners, affiliates and advertisers may [] use cookies, and/or small bits of code called 'one pixel gifs' or 'clear gifs'to make cookies more effective." For purposes of the ECPA claim, the Court agreed with Bresnan that users were notified, and provided express consent to the monitoring of their electronic communications:

"...the Court concludes that through the OnLine Subscriber Agreement, the Privacy Notice and the NebuAd link on Brenan's website, Plaintiffs did know of the interception and through their continued use of Bresnan's Internet Service, they gave or acquiesced their consent to such interception."

Bresnan also successfully used the "consent" defense to obtain dismissal of plaintiff's intrusion upon seclusion claim. Relying on Bresnan's Online Privacy Policy, Subscriber Agreement and disclosure of the NebuAd service via email, the Montana District Court concluded that: "Plaintiffs cannot demonstrate that their expectation of privacy was objectively reasonable."

Bresnan's challenges to the plaintiffs' CFAA claims met with greater resistance. To maintain a CFAA claim under 18 U.S.C. §1030(a), plaintiffs must show that the defendant: (1)

COMPANIES NEED TO TAKE PROACTIVE MEASURES TO DEAL WITH PRIVACY AND DATA SECURITY

Regardless of the direction of litigation and pending legislative reform, all companies need to ensure compliance with currently applicable laws and, ideally, the latest FTC suggestions, industry best practices, and self-regulatory schemes. This should result in a comprehensive privacy and data security program where a single executive is tasked with company-wide implementation, education, monitoring and enforcement:

- Firstly, companies need to audit their privacy and data security practices (annually is recommended), including a tag audit to determine what tracking devices (including Flash cookies and HTML-5) they and third parties have associated with their websites and mobile sites and applications. The company's advertising practices and applicable vendor relationships also need to be examined. All applicable notices and policies should be reviewed. It is recommended that this be done under the direction of legal counsel, with any participating technical consultants and vendors engaged by counsel, to make the results more likely to be privileged.
- The audit results should result in a data collection, use, sharing and storage map, and a clear understanding of all consumer tracking and profiling the company, or others, engage in connection with its sites, ads, content, etc.
- The audit results should then be used to develop a comprehensive strategy to ensure that the company and its business partners and vendors are in compliance with (1) all applicable laws and regulations; and (2) all relevant industry standards and best practices. If applicable, they may also need to apply EU / international laws and standards.
- Ensure that the company's practices, as confirmed by the audit, match up with comprehensive, apparent, and easily understood consumer-facing privacy polices and terms of use; which documents should be crafted to include language that will provide for the kinds of notice and consent, and limitations on remedies and methods of bringing claims; which courts have ruled or suggested may protect against consumer law suits. Counsel should be consulted regarding how to legally institute any material changes to existing policies.
- Best-of-breed data security, especially for sensitive information, should be instituted, which should include protecting against reasonably foreseeable breaches, monitoring, and a plan for dealing with suspected or actual breaches.
- Advertisers and publishers should comply with the July 2009 Cross-Industry Self-regulatory Program for OBA and the Digital Advertising Alliance's ("DAA") OBA Self-regulatory Program Implementation Guide of October 2009 (see www.aboutads.info), and participate in browser "Don't Track" Feature programs.
- Consider using DAA-approved implementation vendors such as Truste, Evidon or Double Verify, which provide compliance, optimization and analytics.
- Institute training and monitoring and create simple tools such as "do and don't" lists for applicable employees and vendors.
- Deal with vendors, clients, advertisers, ad servers and networks, business partners, etc., and ensure that the contacts with these parties include provisions clarifying responsibility and indemnifying your company. Develop a form bank of standard provisions and require their use.
- Be especially aware of cloud computing and outsourcing vulnerabilities, foreign jurisdiction issues and typically insufficient contractual provisions.
- Consider ways to better provide transparency and choice to consumers and implement "privacy by design" as part of the development of any product, service or process that touches on consumer privacy or data security.
- Look into the scope of coverage and exclusions—and cost of—cyber liability and privacy and data security insurance coverage, and consider insurance requirements in this regard for third parties that have access to your or your consumer's data.

intentionally accessed a computer, (2) without authorization or exceeding authorized access, (3) obtained or altered information (4) from a protected computer that (5) resulted in damage to one or more persons during any one-year period aggregating at least $5,000. Bresnan argued that plaintiffs failed to state claims for violations of the CFAA because Brensan had obtained user consent, and therefore there were insufficient allegations of intentional conduct. The plaintiffs countered that any consent provided via the privacy policy was not meaningful, because the opt-out feature permitted users to opt-out of receiving NebuAd's targeted advertisements, but would not prevent the collection and accessing of the data. In contrast to its ruling in favor of Bresnan on the consent defense to the ECPA, the Mortensen Court determined that there was no user consent for "reversal of their privacy settings" for purposes of the plaintiffs' CFAA claims: "For purposes of a 12(b)(6) motion, Plaintiffs have sufficiently alleged that Bresnan's act of tampering with the security and privacy protocols exceeded any authorization that Plaintiffs may have given."

Bresnan also argued that the CFAA claim could not be maintained because the allegations of harm in excess of $5,000 were insufficiently pled. The Montana District Court concluded that the Mortensen plaintiffs' allegations of harm met the requisite pleading standards of the CFAA: "...because defendants caused identical cookies to be placed on plaintiff's computers, unbeknownst to them."

For many of the same reasons, Bresnan's challenge to the plaintiffs' trespass to chattel claim also failed. The Mortensen Court ruled that:

Plaintiffs have granted Bresnan conditional access for purposes of monitoring Plaintiffs' electronic transmissions as well as placing "cookies" on Plaintiffs' computers for purposes of tracking web activity. However, like Plaintiffs' CFAA claim, Bresnan's alleged actions of altering the privacy and security controls on Plaintiffs' computers activity is sufficiently outside of the scope of the use permitted by Plaintiffs. As such, ...Plaintiffs have sufficiently alleged that Bresnan intentionally interfered with the possession of their personal property.

"The court's order demonstrates the importance of terms of use and privacy policies. Defendants need to look at these documents for the basis of potentially winning cases, and companies that have not yet been sued need to revisit their notices, consents, terms of use, end user license agreements and privacy policies with an eye toward including language that will best create defenses to the types of claims that are becoming common in OBA cases. Indeed, while the Bresnan privacy policy and terms of use were effective in warding off some claims, they lacked language that might have fettered the other claims."

On February 11, 2010 the same plaintiffs' law firms that filed the complaint in the Green and Mortensen matters filed a complaint against Centurytel, Inc., another commercial ISP. The case, titled Deering v. Centurytel, Inc., et al. 1:10-cv-00063 (District of Montana) is a mirror image of the Green and Mortensen class actions. In light of the Montana District Court's dismissal of the ECPA and intrusion upon seclusion counts in the Mortensen class action, Centurytel filed a similar motion to dismiss on January 25, 2011. Centurytel argued that (like the defendant in the Mortensen case), Centurytel notified consumers of the possibility of monitoring their activities and sharing data with third party advertisers through its privacy policy and other customer communications. The Court granted the motion to dismiss on May 16, 2011. In so doing the Court reasoned that: "As this Court noted in Mortensen v. Bresnan Communications, consent is a defense to ECPA and invasion of privacy claims. Since Deering acquiesced his consent by using CenturyTel's services knowing his Internet activity could be diverted and used to target him with advertisements, the motion must be granted."

The Website Cases

There are several class actions pending against Facebook that have been consolidated into one action in Northern District of California before Judge Ware. The plaintiffs have filed separate class actions, but their claims are based upon alleged violations of the ECPA, CFAA and state law for the disclosure of a user's unique Facebook ID number. Plaintiffs contend that if a person knows the user ID number or "username" of an individual who is a user of Defendant's website, that person can see the user's profile and see the user's real name, gender, picture, and other information.

The plaintiffs contend that Facebook "serves more ad[vertisement] impressions than any other online entity," and that because it possesses personal information about its users, Defendant's advertisers are able to target advertising to users of Defendant's website. Plaintiffs claimed that Facebook's policies prohibit Defendant from revealing any user's "true identity" or specific personal information to advertisers. Plaintiffs object to the fact that when they click on an adverti-

sement posted on the website, Defendant sends a "Referrer Header" to the corresponding advertiser. This Referrer Header reveals the specific webpage address that the user was looking at prior to clicking on the advertisement. Thus, Plaintiffs allege Defendant has caused users' Internet browsers to send more information to advertisers that it is permitted.

Defendants brought a motion to dismiss on the grounds that plaintiffs had failed to show injury or harm, among other things. The plaintiffs argued that the statutory violations of privacy constituted harm. On May 12, 2011, Judge Ware disagreed, dismissing the plaintiffs' ECPA claims with leave to amend. Judge Ware's decision is consistent with a similar ruling that was made in the Central District in another case.

In addition, as discussed above, since January, 2011, some 20 additional class action complaints have been filed against numerous companies such as Nordstrom, Metacafe, Phillips Electronics of North America, YouTube, Skype, TV Guide Online Holdings, BuySafe, Pandora Media, E*Trade Financial Corp, C3 Metrics, ShopLocal, Google, Apple, Skechers USA, Reebok International, and Amazon among many others. Each of these complaints differs from the earlier ISP cases in that direct allegations are made against the website publisher for use of device identifiers such as so-called Flash cookies to serve targeted ads. A Flash cookie (or Flash local shared object) is a unique form of data file that is stored on a consumer's computer. Flash cookies are stored in areas of the computer not controlled by the browser, which has been the impetus for many of the complaints: consumers are alleged to generally understand that they can use browser tools to control cookies and tracking and, accordingly, tracking devices that circumvent these tools are alleged to be deceptive and unfair. These cases remain in the early stage.

The recent decisions in the Facebook, Green and Mortensen cases are instructive for these pending website cases. Emerging as important trends for defendants are motions to dismiss to challenge the named plaintiffs' (1) standing; (2) consent to tracking and targeted advertising; and (3) alleged damages under the CFAA. Also, as CFAA claims proceed to trial, some defendants may be able to argue that they did not intentionally access or track user behavior, because their websites were enabled by vendors and not the company itself. Also, the dormant commerce clause might emerge as a defense that defendants will use to prevent decisions in one case from creating a de facto national policy regarding behavioral tracking.

The Mobile Cases

On September 16, 2010, Ringleader Digital, a mobile web advertising company, and many of its clients were hit with a proposed class action lawsuit over its use of software code—HTML5—to track iPhone and iPad users across a number of websites. The case, styled Aughenbaugh v. Ringleader Digital, Inc., CNN, Inc., Travel Channel LLC, et al., was originally filed in the Central District of California, but was transferred on February 16, 2011 to the Southern District of New York. It has been consolidated with a related litigation. The case is believed to be the first privacy lawsuit of its kind in the mobile space focusing on tracking for targeted advertising.

In another case involving widgets and other downloadable applications styled White v. Clearspring Technologies, Disney Internet Group, Warner Bros. Records et al. (C.D. Cal. August 10, 2010), Clearspring Technologies and several of its clients were sued for the use of tracking devices to track user behavior online when widgets or other applications are downloaded by the user either on mobile devices or computers. The case was consolidated with a similar and previously filed action titled Valdez v. Quantcast, MTV, NBC Universal et al (C.D. Cal. July 23, 2010). In December 2010, the case was settled for $2.4 million. The electronic distributor Videoegg joined the settlement, bringing the value up to $3.25 million. However, no proceeds from the settlement will go to class plaintiffs.

Other Developments

Equally important in this discussion is the Supreme Court's recent decision regarding the enforceability of consumer arbitration clauses. On April 27, 2011, in the ATT Mobility v. Concepcion case, the U.S. Supreme Court held that the Federal Arbitration Act required California to enforce arbitration agreements even if the agreement requires that consumer complaints be arbitrated individually (instead of on a class-action basis), and preempted California law to the contrary. This decision has significant implications for website operators that include arbitration clauses in their terms of use which expressly limit or prevent consumers' abilities to pursue class-wide relief. The enforceability of consumer facing arbitration provisions has been an issue in flux over the past several years, but the Supreme Court's 5-4 decision seems to resolve the question.

Although the state of the law is in progress, 2011-12 promises to bring decisions that will define the scope and reach of behavioral advertising class actions.

POTENTIAL LEGISLATION

This year has seen numerous federal bills introduced or drafted for potential introduction. Jackie Spier has offered bills regarding both a Do Not Track requirement and financial privacy. Bobby Rush has proposed comprehensive privacy legislation. Jay Rockefeller has jumped on the Do Not Track bandwagon with his own bill. Representatives Ed Markey and Joe Barton have released a draft bill that would impose Do Not Track for children and teens and would require an "eraser button" to eliminate publicly available information. Senator Al Franken has been holding hearings on consumer data privacy and data security relating to mobile devices and may propose language specific to concerns unique to those issues, including problems regarding user location information. Of all the currently proposed federal legislation, a bill by Senators Kerry and McCain seems to have the most traction. It provides for a required notice and opt-out of tracking and targeting rather than a requirement of prior consumer consent, and requires baseline privacy protections for consumers—including transparency, choice and security. One controversial aspect of the bill is that it would make UDID, the unique identifiers assigned to mobile devices, personally identifiable information. Importantly, many of the proposed federal bills would preempt state law and do not have a private right of action. This is important, as a pending California Do Not Track bill provides for $1,000 statutory penalties per violation and a private right of action. Another California bill that would have required that all social networks provide a default privacy setting that makes user profile information private unless the user consents to specific forms of sharing recently lost by two votes.

The Obama administration has announced that passing of legislation for both a federal consumer data privacy scheme and a federal data security and breach remediation scheme is a priority. The degree of interest in these issues by consumer groups, legislators and the media make it more likely than ever that we will see federal legislation on these issues pass in the next year or two. It is essential to the media and entertainment industry that any such legislation strike the proper balance between consumer protection and the ability of content owners and advertisers to adequately monetize new media, which has disrupted their traditional methods of distribution and advertising.

STEPS COMPANIES CAN TAKE NOW

Any company that advertises online or via mobile device, has a website or mobile site or application, or otherwise collects, uses or stores consumer data must have a through understanding of its current policies and practices, ensure that it is complying with current law, get ahead of potentially bad legislation by joining industry self-regulation efforts, join the debate in Washington and in state capitals, and take proactive steps to minimize their risk of claims and to have defenses and remedies if claims are brought. It is recommended that expert privacy and data security counsel be sought, and that a single senior executive be tasked company-wide to address these issues—a position that has become known at many companies as a Chief Privacy Officer. The break-out box contained in this article provides more specific advice on what forward-thinking companies should be doing now.

AUTHOR PROFILE

DOMINIQUE **SHELTON**

Dominique Shelton is a partner in the Intellectual Property department of Wildman Harrold's Los Angeles office. Her practice focuses on complex commercial litigation with a particular concentration in the areas of unfair competition, intellectual property and antitrust. Dominique has represented Fortune 500 companies, start up ventures, and privately held companies in litigation involving advertising, technology, entertainment and software industries. Her representative clients include original equipment manufacturers, television and film studios, cable channels, technology companies, semiconductor distributors, and major arts institutions in Los Angeles. Dominique has a broad range of experience in technology and intellectual property issues particularly in the areas of digital distribution and new media. She advises advertisers, product manufacturers, and cable studios regarding privacy, regulatory issues arising from Web 2.0 marketing, behavioral advertising, social networking websites, user-generated content, and digital advertising.

Contact: Dshelton@Wildman.com

AUTHOR PROFILE

ALAN **FRIEL**

Alan Friel is the Guest Editor of this Insights publication. Please see page 5 for his full biography.

Contact: Friel@Wildman.com

RECENT FTC ENFORCEMENT ACTIONS INVOLVING ENDORSEMENTS, PRIVACY AND DATA SECURITY

By James Taylor & Jill Westmoreland

» ENDORSEMENTS

The Federal Trade Commission (FTC) revised its Guides Concerning the Use of Endorsements and Testimonials in Advertising ("Guides") in December 2009 to, among other things, update the Guides with regard to social media marketing. Since the revised Guides were issued, the FTC has announced the settlements of two enforcement actions involving online reviews. Both involved reviews of products that appeared to be "independent" but were in fact provided by individuals with connections to the product's distributor. The FTC's endorsement guidelines require a reviewer to disclose a material connection with the seller of the product being reviewed.

Legacy Learning System agreed to settle FTC charges that it deceptively advertised its guitar lesson DVDs through online affiliate marketers who falsely posed as ordinary consumers or independent reviewers. The FTC charged that Legacy Learning disseminated deceptive advertisements by representing that online endorsements written by affiliates reflected the views of ordinary consumers or "independent" reviewers, without clearly disclosing that the affiliates were paid for every sale they generated.

Under the proposed settlement, Legacy Learning will pay $250,000. In addition, it must monitor and submit monthly reports about its top 50 revenue-generating affiliate marketers, and make sure that they are disclosing that they earn commissions for sales and are not misrepresenting themselves as independent users or ordinary consumers. Legacy Learning also must monitor a random sampling of another 50 of their affiliate marketers, and submit monthly reports to the FTC about the same criteria.

The FTC suggests that advertisers using affiliate marketers to promote their products should put a reasonable monitoring program in place to verify that those affiliates follow the principles of truth in advertising.

The FTC announced a settlement with Reverb Communications, Inc., a company that provides public relations, marketing, and sales services to developers of video game applications, including mobile gaming apps. Reverb employees posted reviews about their clients' games at the iTunes store using account names that gave readers the impression the reviews were written by disinterested consumers, according to the FTC complaint. The company did not disclose that it was hired to promote the games and that the reviewers often received a percentage of the sales.

Under the proposed settlement order, Reverb and its sole owner are required to remove any previously posted endorsements that misrepresent the authors as independent users or ordinary consumers, and that fail to disclose a connection between Reverb and the seller of a product or service. The agreement also bars Reverb from misrepresenting that the user or endorser is an independent, ordinary consumer, and from making endorsement or user claims about a product or service unless they disclose any relevant connections that they have with the seller of the product or service.

These two enforcement actions are a reminder that the FTC is monitoring how companies market products online and, in particular, in blogs and other forms of social media. Companies that post online reviews, or engage others to post reviews, should consult the FTC's endorsement Guides. The Guides state that bloggers should disclose any material connection with an advertiser, and that endorsements should not contain false or misleading statements. The advertiser as well as the blogger can be liable for false or misleading statements made in social media. The FTC suggests that advertisers provide guidance to bloggers and should monitor blogs to see that bloggers are not making false or misleading statements. The Guides also address celebrity endorsements: celebrities can be liable for false or misleading statements, so advertisers engaging celebrity endorsers should make sure endorsers are familiar with the products and services they are promoting.

» PRIVACY

The FTC continues to be the most active regulatory agency when it comes to privacy and data collection. The FTC's primary enforcement tool is Section 5 of the FTC Act, which prohibits unfair or deceptive acts or practices in commerce. For over a decade, the FTC has charged companies that fail to comply with their own privacy promises as violating Section 5 of the FTC Act.

In March 2011, the FTC announced that online advertising company Chitika, Inc. agreed to settle charges that it engaged in deceptive advertising by tracking consumers' online activities even after they opted-out of online tracking on Chitika's website. According to the FTC's complaint, Chitika buys ad space on websites and contracts with advertisers to place small text files (cookies) on those websites. The FTC alleged that in its privacy policy the company says that it collects data about consumers' preferences, but allows consumers to opt out of having cookies placed on their browsers and receiving targeted ads. The privacy policy includes an "Opt-Out" button. Consumers who click on it activate a message that states, "You are currently opted out."

According to the FTC, Chitika's opt-out lasted only ten days. After that time, Chitika placed tracking cookies on browsers of consumers who had opted out and targeted ads to them again. The FTC charged Chitika's claims about its opt-out mechanism contained in its privacy policy were deceptive and violated federal law. The settlement bars Chitika from making misleading statements about the extent of data collection about consumers and the extent to which consumers can control the collection, use or sharing of their data. It requires that every targeted ad include a hyperlink that takes consumers to a clear opt-out mechanism that allows a consumer to opt out for at least five years. It also requires that Chitika destroy all identifiable user information collected when the defective opt-out was in place. In addition, the settlement requires that Chitika alert consumers who previously tried to opt out that their attempt was not effective, and they should opt out again to avoid targeted ads.

In March 2011, Google settled FTC charges that it engaged in deceptive tactics and violated its own privacy promises when it launched its social network called Buzz, which disclosed users' contacts. The FTC alleged that Google violated its own privacy policy by disclosing users' contacts without permission, and Google failed to adequately describe how users' information would be disclosed. The FTC stated that this was the first FTC settlement in which a company agreed to implement a comprehensive privacy program to protect the privacy of consumer data. Google also agreed to independent privacy audits for the next 20 years.

These are just two of hundreds of enforcement actions the FTC has initiated against companies that failed to act in accordance with their own privacy policy. Companies need to examine their data collection, use, and disclosure practices carefully. Companies that provide a privacy policy need to accurately describe their privacy practices, and update that policy to reflect any changes. In addition, companies should confirm that software or third-parties they use to process opt-outs are working properly.

» DATA SECURITY

The FTC also monitors whether companies are providing reasonable security for data they collect, store, and share. Two recent settlements highlight the importance of implementing security measures to protect employee, client and consumer data. In these actions, the FTC charged that both companies claimed they would take reasonable measures to secure the consumer data they maintained, including Social Security numbers, but failed to do so. These flaws were exposed when security breaches at both companies put the personal information of thousands of consumers at risk. The FTC challenged the companies' security practices as unfair and deceptive.

According to the FTC's complaint against Ceridian Corporation, a provider to businesses of payroll and other human resource services, the company claimed, among other things, that it maintained "Worry-free Safety and Reliability... Our comprehensive security program is designed in accordance with ISO 27000 series standards, industry best practices and federal, state and local regulatory requirements." The FTC claimed the company's security was inadequate: among other things, the company did not adequately protect its network from reasonably foreseeable attacks and stored personal information in clear, readable text indefinitely on its network without a business need.

These security lapses enabled an intruder to breach one of Ceridian's web-based payroll processing applications and obtain the personal information—including Social Security numbers and direct deposit information—of approximately 28,000 employees of Ceridian's small business customers.

Lookout Services, Inc., markets a product that allows employers to comply with federal immigration laws. It stores information such as names, addresses, dates of birth and Social Security Numbers. According to the FTC's complaint, despite the company's claims that its system kept data reasonably secure from unauthorized access, it did not in fact provide adequate security. For example, unauthorized access to sensitive employee information allegedly could be gained without the need to enter a username or password, simply by typing a relatively simple URL into a web browser.

In addition, the complaint charged that Lookout failed to require strong user passwords, failed to require periodic changes of such passwords, and failed to provide adequate employee training. As a result of these and other failures, an employee of one of Lookout's customers was able to access sensitive information maintained in the company's database, including the Social Security numbers of about 37,000 consumers.

According to the FTC's press release, these two settlements are part of the FTC's ongoing efforts to ensure that companies secure the sensitive consumer information they maintain. They also illustrate the consequences of failing to provide adequate security: both companies are required to implement a comprehensive information security program and to obtain independent, third party security audits every other year for 20 years.

THE FTC PROVIDES A WEALTH OF RESOURCES RELATING TO ENDORSEMENTS, PRIVACY AND DATA SECURITY. HERE ARE JUST A FEW:

THE FTC'S REVISED ENDORSEMENT GUIDES:
What People Are Asking
http://business.ftc.gov/documents/bus71-ftcs-revised-endorsement-guideswhat-people-are-asking

SOCIAL STUDIES:
Applying the FTC's Revised Endorsement Guides in New Marketing Media
http://business.ftc.gov/documents/social-studies-applying-ftcs-revised-endorsement-guides-new-marketing-media

WHEN YOU WISH UPON A STAR:
Celebrity Endorsements & the FTC's Revised Endorsement Guides
http://business.ftc.gov/documents/when-you-wish-upon-star-celebrity-endorsements-ftcs-revised-endorsement-guides

PRIVACY POLICIES:
Say What You Mean and Mean What You Say
http://business.ftc.gov/documents/art09-privacy-policies-say-what-you-mean-and-mean-what-you-say

PROTECTING PERSONAL INFORMATION:
A Guide for Business
http://www.ftc.gov/bcp/edu/microsites/infosecurity/

AUTHOR PROFILE

JAMES TAYLOR

James Taylor is a Partner at Loeb & Loeb, Co-Chair of their Advanced Media and Technology Department, and Chair of their Advertising and Promotions Law Practice Group. Mr. Taylor's principal practice areas include advertising, promotions and privacy for advertisers, advertising and promotion agencies, and entertainment, media, Internet and mobile clients. Mr. Taylor counsels clients on their integrated marketing initiatives, agency services agreements, sponsorships and brand integration agreements, vendor and strategic partnership contracts, talent and music agreements, guild issues, social media initiatives, privacy issues including behavioral targeted marketing and data protection policies, software and technology licenses, intellectual property counseling, copy review, sweepstakes and other promotional offers. Mr. aylor is on the Editorial Board of the Advanced Media & Technology Law Blog.

Contact: Jtaylor@loeb.com

AUTHOR PROFILE

JILL WESTMORELAND

Jill Westmoreland is an attorney at Loeb & Loeb with experience in the entertainment and publishing industries. Ms. Westmoreland conducts legal research and writes summaries of judicial decisions, legislation, regulations, enforcement actions and industry developments on a variety of topics including copyright and trademark infringement; advertising, marketing and promotions; and privacy and data security. Ms. Westmoreland is an Editor of the Advanced Media and Technology Law Blog and the Associate Editor of the IP/Entertainment Weekly Case Update for Motion Picture Studios and Television Networks.

Contact: jwestmoreland@loeb.com

APP-ENDECTOMY:
REMOVING THE MYSTERY FROM THE APP ECOSYSTEM[1]

By Wayne M. Josel & Dan Schnapp

A scant three years ago, Apple launched its App Store with 500 apps. There are now well over 350,000 apps available from Apple, 150,000 apps for Android devices, and a rapidly escalating number of apps that can be run on Blackberry OS and other mobile devices and platforms. Clearly, the app industry, currently estimated at $7 billion, is booming. A recent report projects that by 2014, that value will increase to $30 billion, with over 21 billion apps being downloaded.

But with this explosive growth comes considerable challenges. Of paramount concern to app publishers and developers is how to successfully navigate a rapidly evolving ecosystem comprised of multiple stakeholders with divergent interests and offerings, storefronts with inconsistent terms, and devices with different operating systems, platforms and technical requirements. Out of this core challenge, various business, legal, and operational issues arise which must be carefully analyzed and addressed by any entity seeking to develop, publish, distribute, sell and/or exploit apps.

DEVELOPMENT AND DISTRIBUTION ISSUES

Although certain correlations exist when considering the issues related to development and distribution of apps and the development and distribution of other digital media, content, and software, the app economy has undoubtedly given rise to novel issues in these contexts. First, the time to market for apps is extraordinarily fast-paced, and app shelf-life is relatively short. Second, with multiple devices operating on multiple platforms, consumers demand device-agnostic apps with cross-platform compatibility (for example, apps that enable a consumer to store and sync data for access on a Windows-based PC, iPad and Android phone).

Apps generally must undergo a multi-faceted certification and approval process by app storefront/platform operators. Developers and publishers therefore have to take into account the various technical considerations of each app market operator or distributor. Gaining promotional exposure for apps within app storefronts and facilitating consumer discovery of apps within such storefronts are yet other challenges to be addressed. Moreover, the retail channels of distribution vary depending on device. For example, apps for the iPad/iPhone/iPod Touch are available only from the Apple App Store, for which each and every app must be individually

[1] *This article is adapted from a recent CLE-accredited webinar presented by the authors. The webinar and accompanying materials can be accessed at http://digitalhhr.com/webinars/.*

approved by Apple. Android-based apps are available both through Google's Android Market and numerous third parties, lacking any primary approval authority.

Finally, everything from technical specifications, pricing guidelines, restrictions and conditions on advertising, and rights on the collection and use of data are set forth in a myriad of license agreements (*e.g.* SDK and API licenses and terms of service, storefront agreements, EULAs, *etc.*) which are, for the most part, provided on a "click-through", non-negotiable basis. Prudence dictates that each of the applicable agreements be carefully reviewed and analyzed to ensure that the developer/publisher's app business model fits squarely within the terms and conditions established by the entity (or entities) which control the applicable app ecosystem. In most cases, that entity will be the one primarily associated with the device platform on which the app will function (*e.g.* Apple for iPhone, iTouch, iPad and Mac apps, Google for Android apps, *etc.*). A developer/publisher launching a broad, cross-platform app strategy will need to comply with multiple agreements, some of which have inconsistent standards and provisions.

APP BUSINESS MODELS/MONETIZATION INITIATIVES

The app ecosystem provides developers and publishers with multiple opportunities for monetization. The most readily apparent (and straightforward) one is through paid downloads of the app itself. Other revenue opportunities exist through the distribution of "freemium" apps, those that are initially made available with a limited feature and function set as a way to entice consumers to pay for an upgraded version that enables access to all of the app's features and functionality. In addition, some apps can be ad-supported, with banner and display ads being featured in areas adjacent to the app or integrated into the app itself.

In-app purchases and billing provide alternate and incremental revenue opportunities. These can include, among other things, purchases for additional content and features, subscriptions or "off-deck" purchases, made when the app directs the user to an e-commerce website.

Nearly all of these monetization initiatives involve a revenue share between the developer/publisher and app market operator. With respect to paid downloads, with limited exceptions, the app economy seems to have settled on a 70-30 revenue split, meaning that if an app is being sold in a market for $1.00, the developer/publisher gets $0.70 and the app store or market operator retains $0.30 from the sale.

The revenue share model for subscriptions is a bit more complicated. While Apple is requiring the same 70-30 split for subscriptions sold through the iTunes App Store, if a publisher or developer sells a subscription for an iPhone or iPad directly to a consumer (for example on its own website), it shall retain all of the revenue from that sale. Google has not yet launched its subscription-based apps market but early announcements pointed to a revenue split that was more favorable to the developer/publisher than Apple's.

In addition to revenue splits, the app storefront operators have placed other restrictions and conditions on the commercialization of apps. For example, Apple prohibits developers/publishers from providing links in their apps (to a website, etc.) which allow consumers to purchase content or subscriptions outside of the app. Apple recently backed down from its initial position, which would have also prohibited publishers from offering subscriptions sold directly to consumers at a more favorable price than those offered through the App Store. Thus, while publishers are free to offer better terms for subscription content to be viewed on an iPad app on their own website, the app itself can't be used to link directly to that site or offer. Google prohibits develop/publishers from using its Android Market to distribute apps whose primary purpose is to facilitate the distribution of apps outside of the market itself. At first blush, these types of restrictions appear to act primarily to provide uniformity for app pricing and features. However, they also have the collateral effect of restraining businesses from driving traffic to their sites, where valuable data can be collected. The restrictions may therefore hinder the growth of the app market in certain areas. In particular, the magazine publishing industry has shown hesitancy to launch aggressive app initiatives, in part because of obligations and restrictions placed on the publishers' ability to control and use data collected from subscribers and potential subscribers.

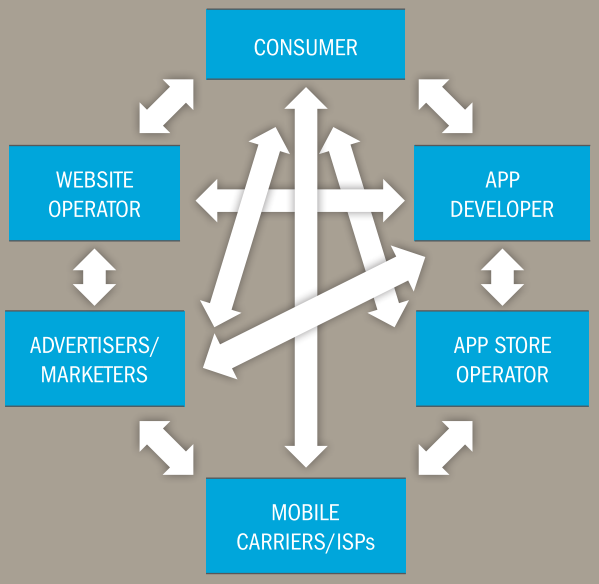
DATA COLLECTION AND PRIVACY ISSUES

The very nature of the app ecosystem—how apps are sold, where they are used, what information is being accessed through them, *etc.*—provides unprecedented opportunities for the collection and exploitation of data. For example, when an app is purchased, a host of personally identifiable information (PII) is collected by the app storefront/platform operator, including the consumer's name, mailing address, e-mail address, credit card information, *etc.* The app storefront/platform operator will also know what type of device the consumer is using and, presumably, knows about every other app he or she purchased through the store. In addition, depending on the functionality of the app, the app developer/publisher may know when the consumer access the app (*e.g.* if the app connects to the developer/publisher server to obtain content) and where he or she is when accessing the app (*i.e.* through an IP address and/or other location-based functionality within the device or app).

Knowing where a consumer lives (either by the exact address or more general location such as zip code), what device he or she uses, and the types of apps he or she purchases can provide a fairly detailed and arguably invaluable profile of that consumer and his or her economic status from a marketer's perspective. That in turn can be used to sell and target ads for products that might be of interest. For example, a consumer from Westchester County, NY who owns an iPad and buys and downloads music-related apps is likely to be interested in concert and theater tickets and other premium items. Knowing that a consumer is in a certain town or neighborhood may enable marketers to push coupons and discounts to local shops and restaurants in real time.

However, the interlocking relationships in the app eco-system complicates the picture (see Sidebar). The multiple stakeholders—developer, publisher (which may or may not be the same entity), app storefront/platform operator, mobile carrier/internet service provider, marketers/advertiser and end users—all have varying, and in some cases competing, interests with respect to the collection and use of data. In addition, since many of the stakeholders are parties to multiple agreements, each with their own terms and conditions related to data disclosure and privacy, determining precisely where the boundaries on use lie can be difficult.

STAKEHOLDER RELATIONSHIP



This graphic represents the various stakeholders in the app ecosystem. Each arrow represents a license/development/distribution or other agreement between the applicable stakeholders, and each agreement will set forth terms and conditions for the collection, use and disclosure of data that is generated in connection with the relationship between the stakeholders.

In many instances the same "basket" of data is governed by provisions in multiple agreements. For example, information collected when an end user purchases an app (*e.g.* account name, mailing and e-mail address, credit card information, name/type of app, cost, location of device when purchase was made, *etc.*) may be accessible by the app store operator, publisher and mobile carrier/ISP. Additionally, information collected when an advertisement in an app is viewed may be accessible by the app publisher, mobile carrier/ISP and advertisers/marketers (as well as any ad serving entity).

Moreover, each of these agreements also contain their own representations, warranties and indemnification provisions. In the event of a data security breach, untangling and apportioning responsibility and/or liability will clearly be a difficult exercise.

It is critical for stakeholders to carefully review and analyze the provisions related to data collection, use, disclosure and privacy that are contained in the various agreements that it will be party to, as well as the reps, warranties and indemnification provisions. Knowing precisely which party has which rights and obligations and how the risks have been allocated across all of the agreements will help ensure that a party can properly tailor its business initiatives and objectives within the legal framework.

As the primary sales point in the app ecosystem, the app storefront/platform operators have established certain guidelines and criteria for data collection, in some instances to widely differing effect. Apple, for example, has implemented relatively strict standards. In the terms and conditions for the distribution of subscription-based apps, Apple requires publishers to clearly and conspicuously notify users of the privacy policy governing the use of the app, effectively implementing an opt-in/opt-out feature. In addition, the publisher must obtain a consumer's express consent before collecting, transmitting or using location-based data, which can only be used when it is directly relevant to the features and services provided by the app or to support approved advertising uses. Some publishers have already expressed concern that many subscribers will opt-out of the data collection process, denying the publishers the opportunity to sell high-value ads based on the kinds of granular data that can be collected through an app. However, recent forays by publishers like Conde Nast, which has recently commenced offering The New Yorker through the iTunes Store may be evidence that publishers are becoming more accustomed to Apple's terms (or at least recognizing that there are substantial opportunities even with the restrictions in place).

In contrast, while Google requires publishers using the Android Market to establish a privacy policy and enable customers to opt-out of having his or her personal data shared, it has not placed extensive restrictions on publishers with respect to the sales of ads in their apps. A recent announcement by a consortium of publishers, which will be offering magazine subscriptions to owners of the Samsung's Android-based Galaxy tablet, appears to be the first major move by the magazine publishing industry into the Android eco-system.

This difference in approach is not surprising when one considers the differences in the core businesses of Apple and Google. Apple has historically been a consumer-focused company that has touted its premium products and services. Its approach is intended to protect its relationship with its customers who have purchased its products and used its App Store. Google was (and to date remains) primarily an advertising company. It therefore has a considerably greater interest in enabling and promoting new advertising initiatives through apps on the Android platform than it does in implementing standards that might restrict such initiatives.

TAKE-AWAYS

So what does all of this mean? If pressed to identify the key issue in the app ecosystem, we would have to say "privacy." The potential value that can be extracted from data that could be made available, the interlocking—and at times competing—interests among the stakeholders with respect to the collection, use and disclosure of information, and the potential legal exposure that could result from a data security and privacy breach, are a potent mix.

Stakeholders should chart a course of developing and implementing "best practices" and policy guidelines to govern their approach to privacy issues. These should include clearly defined disclosure to consumers of their privacy policies, as well as heightened consent provisions where applicable.

While the federal government has yet to implement a regulatory scheme to govern the collection, use and disclosure of consumer information, that may change in the future. Each data security breach that makes headlines, including the recent ones involving Sony and Epsilon, makes it more likely that regulations of some sort are in the offing in the future. The various reports on self-regulation and statements and proposals that have been released by the FTC to date can provide substantial guidance on how to frame and deploy "best practices" and robust privacy policies.

More broadly, stakeholders must take a proactive approach to the entire app lifecycle. As should now be apparent, each of the steps in that lifecycle, from concept to development to approval to publication to distribution to marketing, has its own potential pitfalls that could seriously damage not only the specific app initiative, but also have ramifications on a stakeholder's broader business and operations. It is important for stakeholders to seek competent counsel that is intimately familiar with the environment and can efficiently, effectively and creatively craft solutions to not only avoid the pitfalls, but maximize the opportunities for success. It is clear that the app ecosystem is in its infancy. The coming months and years will likely reveal maturation and change as opportunities are pursued and certain initiatives fail while others become wildly successful. But being in a position to exploit the opportunities that will inevitably come requires a comprehensive understanding and appreciation of the landscape as it exists now since no one wants to try to play catch-up in this rapidly-evolving environment.

AUTHOR PROFILE

DAN **SCHNAPP**

Dan Schnapp is a Partner at Hughes Hubbard and Chair of their New Media, Entertainment and Technology Practice. Mr. Schnapp provides strategic counsel and transactional support for multi-national corporations, mid-cap and start-up companies in connection with a wide range of legal and policy issues arising out of the convergence of technology, advertising, entertainment and media and electronic commerce, intellectual property, privacy, information security, compliance and risk management. Mr. Schnapp writes and lectures extensively on new developments in the areas of digital content distribution and syndication, cloud–based content distribution models, end user generated content and social networking initiatives, outsourcing, electronic commerce, electronic payment systems, privacy and information security. Mr. Schnapp was selected in 2008 as one of the "Top 50 IP Attorneys Under 45" in IP Law and Business Magazine.

Contact: Schnapp@hugheshubbard.com

AUTHOR PROFILE

WAYNE M. **JOSEL**

Wayne M. Josel is Counsel in the New Media, Entertainment and Technology group at Hughes Hubbard & Reed LLP. Wayne's practice focuses on the legal, strategic and policy issues arising out of the convergence of technology, entertainment and media. He provides counsel and transactional support in connection with client initiatives related to electronic commerce, intellectual property, privacy, information security, compliance and risk management. He has written extensively, as well as produced and participated in continuing legal education programs, on issues related to cloud computing, TV Everywhere initiatives and privacy. He has moderated panels at the Digital Hollywood East conference and at ACG New York. Wayne is also a member of the Executive Committee of the Digital Media Division of UJA-Federation New York.

Contact: josel@hugheshubbard.com

social networking:
why can't we be friends?

By Julia R. Harris

May a judge be a "friend" on a social network with a lawyer who appears as counsel in a case before the judge?

This question has been posed to lawyers over and over again throughout the last five years, as the online social network has grown. A few states have answered the question, but those answers are far from uniform.

A recent study found that four out of ten judges use social media sites like Facebook and LinkedIn—about the same proportion as the general population.

The Supreme Court of Ohio's disciplinary board decided that judges may use Twitter and "friend" lawyers who appear before them. The advisory opinion from the Board of Commissioners on Grievances & Discipline advised judges that social media use is permitted but must be handled with caution.

Opinion 2010-7 states: "As with any other action a judge takes, a judge's participation on a social networking site must be done carefully in order to comply with the ethical rules in the Code of Judicial Conduct."

The judge must be careful about how much interaction she has with such "friends," and how much information the judge herself lets others see on her own page. Essentially, the Ohio Supreme Court left it up to the judges to decide how much interaction is too much. As we all know, trying to really measure or control Facebook "lurking" is impossible.

As attorneys, we need to protect our reputations—and our ethics, as well. Other noteworthy cautions judges must take, according to the Ohio Supreme Court, include:

- Do not comment on Facebook about other judges' cases before they have reached a decision;
- Be careful with photo, status, and post comments;
- Don't go on a witness' or party's personal profile to obtain information about them or the cause of trial.

Lawyers would do well to heed the same advice, even if they practice in a state that has not reached an opinion as Ohio did.

Kentucky, New York and South Carolina maintain that "friending" on social media does not imply that the friend has special "pull," but that it may (in some circumstances) rise to the level of a "close social relationship," mandating disclosure to opposing counsel, and sometimes even recusal.

In other states (Florida, for example), judges are prohibited from "friending" a lawyer because it could convey the impression that the lawyer is in a special position to influence the judge.

Florida's Judicial Ethics Advisory Committee found that judges cannot accept friend requests from litigants in their court. The court stressed that the opinion is limited to lawyers who may appear before the judge. Therefore, the opinion does not apply to the practice of friending persons other than lawyers, or to friending lawyers who do not appear before the judge, either because they do not practice in the judge's area or court or because the judge listed them on her recusal list so that their cases are not assigned to the judge.

Although Facebook was used as an example in this opinion, the holding applies to any social networking site which requires the member of the site to approve the listing of a "friend" or contact on the member's site, if (1) that person is a lawyer who appears before the judge, **and** (2) identification of the lawyer as the judge's "friend" is thereafter displayed to the public or the judge's or lawyer's other "friends" on the judge's or the lawyer's page.

what about twitter?

If someone is protected on Twitter, he has to approve all followers. Anybody can see which followers have been approved. Does that constitute identification as a "friend" on the judge's page? I think that it might. Even if you are an attorney in a state that does allow social networking between judges and lawyers, you would be well-advised to think twice before "friending" a judge. Remember, everything that you put on the Internet potentially stays there forever. Do you really want a judge that you appear before to see pictures of your bachelor/bachelorette weekend in Vegas? What happens in Vegas is supposed to stay in Vegas. However, with Facebook and Twitter, what happens in Vegas may make it before the eyes of a relevant judge!

Minions of the law, rest at ease: lawyers can declare themselves Facebook "fans" of judges, the committee said, "as long as the judge or committee controlling the site cannot accept or reject the lawyer's listing of himself or herself on the site."

You might be thinking that a person who is on Facebook might have dozens, hundreds, or even thousands of Facebook friends. Thus being a Facebook "friend" conveys very little, least of all that it suggests that certain attorneys have cozy relationships with a judge, and therefore have the power to influence his or her decisions. But consider this: the North Carolina state judicial standards commission publically reprimanded Judge B. Carlton Terry Jr. for discussing a custody matter on Facebook with a lawyer. The limited conversation constituted a violation of the ex parte prohibition. There is no telling what sort of sanctions could be imposed on an attorney for the ex parte communications in another state. The lesson here is to refrain from discussing any legal matter with a judge via a social networking site, and in fact, avoid the danger all together by simply not "friending" a judge if you are a lawyer.

what if you were friends with the judge before she became a judge?

The states that have ruled against judges and lawyers being friends on social networking sites established that judges may not friend lawyers who appear before the court. However, what if a lawyer "friended" a judge before she was a judge? As of the writing of this article, it appears that question has not been answered by any ethics committee in any state. However, in the days before Twitter and Facebook, a good friend of a judge would likely be on the recusal list. Therefore, if a lawyer was good enough friends with a judge before she was a judge to be friends with her on a social networking site, she likely would end up on the recusal list post-appointment.

In any case, if you find yourself in front of a judge with whom you are good friends, or even if you are simply Facebook friends, that information should be revealed to opposing counsel. An even safer bet: defriend the judge! I'm sure she will understand, and you may in fact beat her to the punch.

disclosure of confidential information

Lawyers have a fiduciary duty to protect their client's confidential information. In California, client's confidential information was originally protected only through the State Bar Act. However, there is now also an ethics rule covering client confidentiality.

Confidences include all information learned during the course of the attorney/client relationship, information related to the representation, and all information relating to the representation, any of which might be embarrassing or detrimental to the client if disclosed.

Publicly-known information can still be a client confidence. Information does not need to come from the client in order to be considered confidential information. As you can see, the breadth of what counts as a client's confidential information is wide and deep, and in reality it is almost all information relating to the representation. Therefore, lawyers must maintain a higher level of confidentiality than most professions. Attorneys do not need to use names or specific details in order to break confidentiality.

We know that lawyers can be garrulous. We love to brag about interesting cases we are working on, swap war stories, and do our version of name-dropping by revealing our prestigious clients. Those disclosures were traditionally made in the course of private, oral discussions among professional colleagues. Social networking sites changed all of that. Expectation of privacy in social networking is extremely reduced, and once words are posted on the Internet, they will be public forever.

It is paramount to disclose who your Facebook friends are, whom you are Linkedin with, and other online connections you may have. Separating personal and business relationships is difficult. If an attorney must have a Facebook or Twitter account in order to, for example, market herself and maintain professional relationships, she should never discuss cases or information related to client work. Instead, she would be wise to focus on getting across her personality traits that make her a good attorney.

Keep your connections updated about your activities. Sharing personal information such as photos of family members and opinions on current events is also a good way to promote your brand while maintaining a high level of client confidentiality.

Social media isn't going anywhere. Being successful, especially in this economy, requires social media savvy and self-branding. However, lawyers need to be especially wary of the information they are putting out into cyber space—forever.

conclusion

The American Bar Association's 2010 Legal Technology Report found that 56 percent of attorneys have a presence in online social networks. Being an attorney with an online social networking presence is not a violation of ethics regulations. However, we would all be well-advised to think twice before launching a message into cyberspace, especially if it is a message to a judge or it includes information regarding one's client. In fact, if an attorney wants to be safe, the better bet is to refrain from even "friending" a member of the judiciary—or posting about a current case at all!

AUTHOR PROFILE

JULIA **HARRIS**

Julia Harris is currently an associate at Kleinman and Associates in Encino. She graduated in May 2010, and was admitted to the California State Bar in December 2010. While in law school, Ms. Harris was a member of the Intellectual Property Law Association, Moot Court Board, and served as the Vice Magister of Golden Gate University's chapter of Phi Delta Phi.

Previously, Ms. Harris interned for the Assistant General Counsel of Paramount Pictures in 2008, and served as a law clerk at Berman Entertainment and Technology Law in San Francisco.

Before entering law school, Ms. Harris spent two years as an associate producer and coordinator in entertainment marketing. She associate produced marketing featurettes for *Cars, Desperate Housewives, Grey's Anatomy,* and *Scrubs.* She also associate produced *The History of New Line Cinema,* a feature-length documentary, as well as Mattel and Intel commercials.

Ms. Harris received a B.A., *cum laude,* in English from the University of Hawaii, Manoa in 2005 and a J.D. from Golden Gate University School of Law in 2010. Ms. Harris serves as the managing editor of *Insights*, and is a member of the Beverly Hills Bar Association, the Los Angeles Bar Association, and an Associate of the Los Angeles Copyright Society.

Contact: Harrisjulia56@gmail.com

Before it hits the fan.

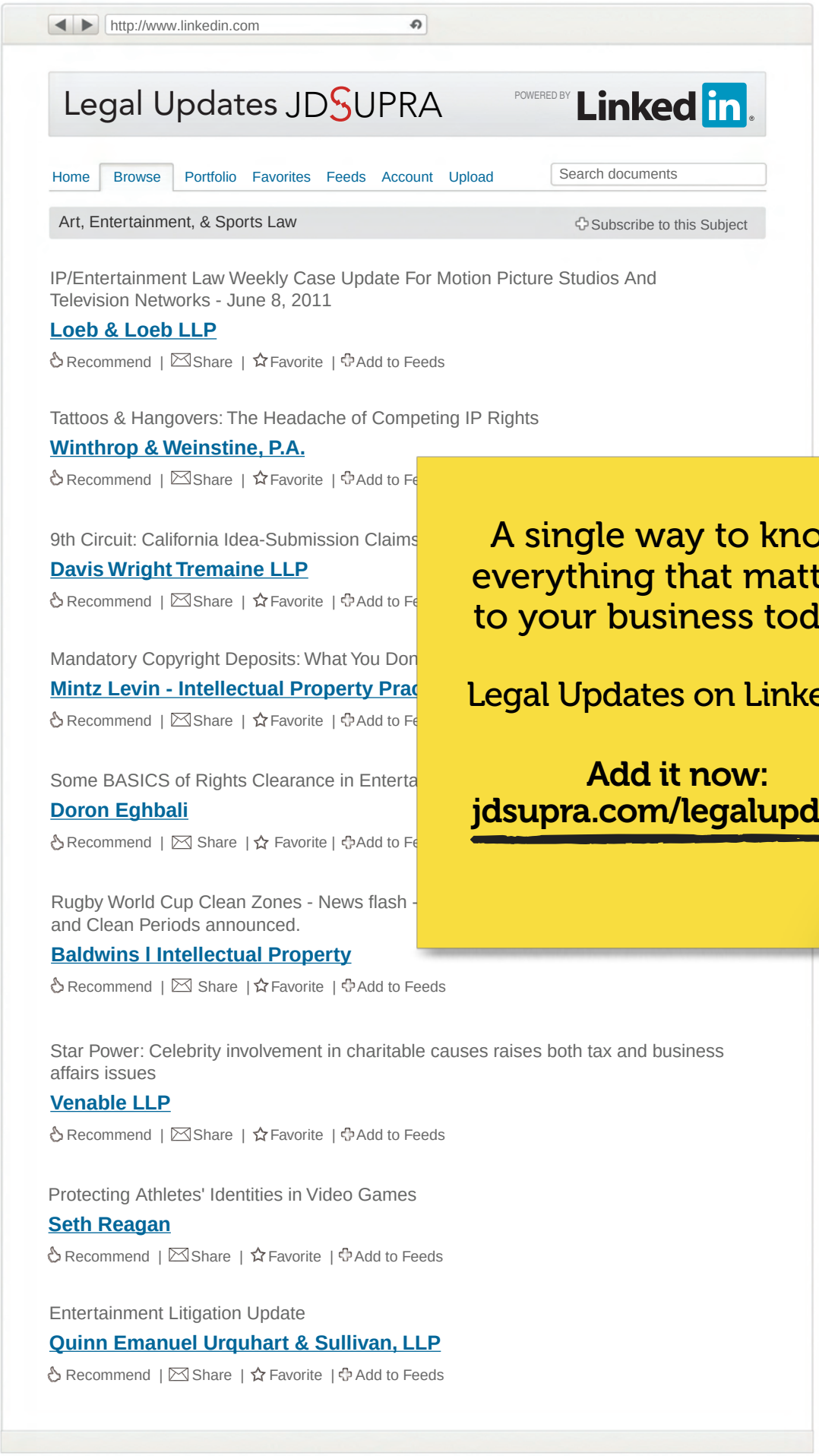
Have you noticed that a large and thriving industry has developed around crisis management? We lead a very small and very different industry; crisis prevention. **Core Strategy Group** is in a category of one; preaching and practicing the discipline of insurgent strategy, learned from the successes of underdogs and revolutionaries in business, politics and warfare. Our four month crisis prevention program helps you and your company see trouble *before* it happens ... our early warning networks smell smoke *before* the flames erupt. Our insurgent strategy training will help you develop a faster, more aggressive and more focused organization, ready for anything.

The Discipline of Insurgent Strategy

If you want a crisis managed – you have lots of choices.

If you want it prevented ... contact Michael Harbert of Core Strategy Group/West.

Michael.Harbert@CoreStrategyGroup.com


http://www.linkedin.com
Legal Updates JDSUPRA
POWERED BY LinkedIn
Home
Browse
Portfolio
Favorites
Feeds
Account
Upload
Search documents
Art, Entertainment, & Sports Law
Subscribe to this Subject
IP/Entertainment Law Weekly Case Update For Motion Picture Studios And Television Networks - June 8, 2011
Loeb & Loeb LLP
Recommend | Share | Favorite | Add to Feeds
Tattoos & Hangovers: The Headache of Competing IP Rights
Winthrop & Weinstine, P.A.
Recommend | Share | Favorite | Add to Fe
9th Circuit: California Idea-Submission Claims
Davis Wright Tremaine LLP
Recommend | Share | Favorite | Add to Fe
Mandatory Copyright Deposits: What You Don
Mintz Levin - Intellectual Property Prac
Recommend | Share | Favorite | Add to Fe
Some BASICS of Rights Clearance in Enterta
Doron Eghbali
Recommend | Share | Favorite | Add to Fe
Rugby World Cup Clean Zones - News flash - and Clean Periods announced.
Baldwins I Intellectual Property
Recommend | Share | Favorite | Add to Feeds
Star Power: Celebrity involvement in charitable causes raises both tax and business affairs issues
Venable LLP
Recommend | Share | Favorite | Add to Feeds
Protecting Athletes' Identities in Video Games
Seth Reagan
Recommend | Share | Favorite | Add to Feeds
Entertainment Litigation Update
Quinn Emanuel Urquhart & Sullivan, LLP
Recommend | Share | Favorite | Add to Feeds
A single way to know everything that matters to your business today:
Legal Updates on LinkedIn
Add it now:
jdsupra.com/legalupdates

Navigating the new media landscape

Wildman Harrold's Media & Entertainment attorneys are highly regarded for their depth of knowledge of the unique legal and business issues specific to the integrated marketing and promotion industry, particularly with the cutting edge issues associated with online, interactive and mobile marketing initiatives.

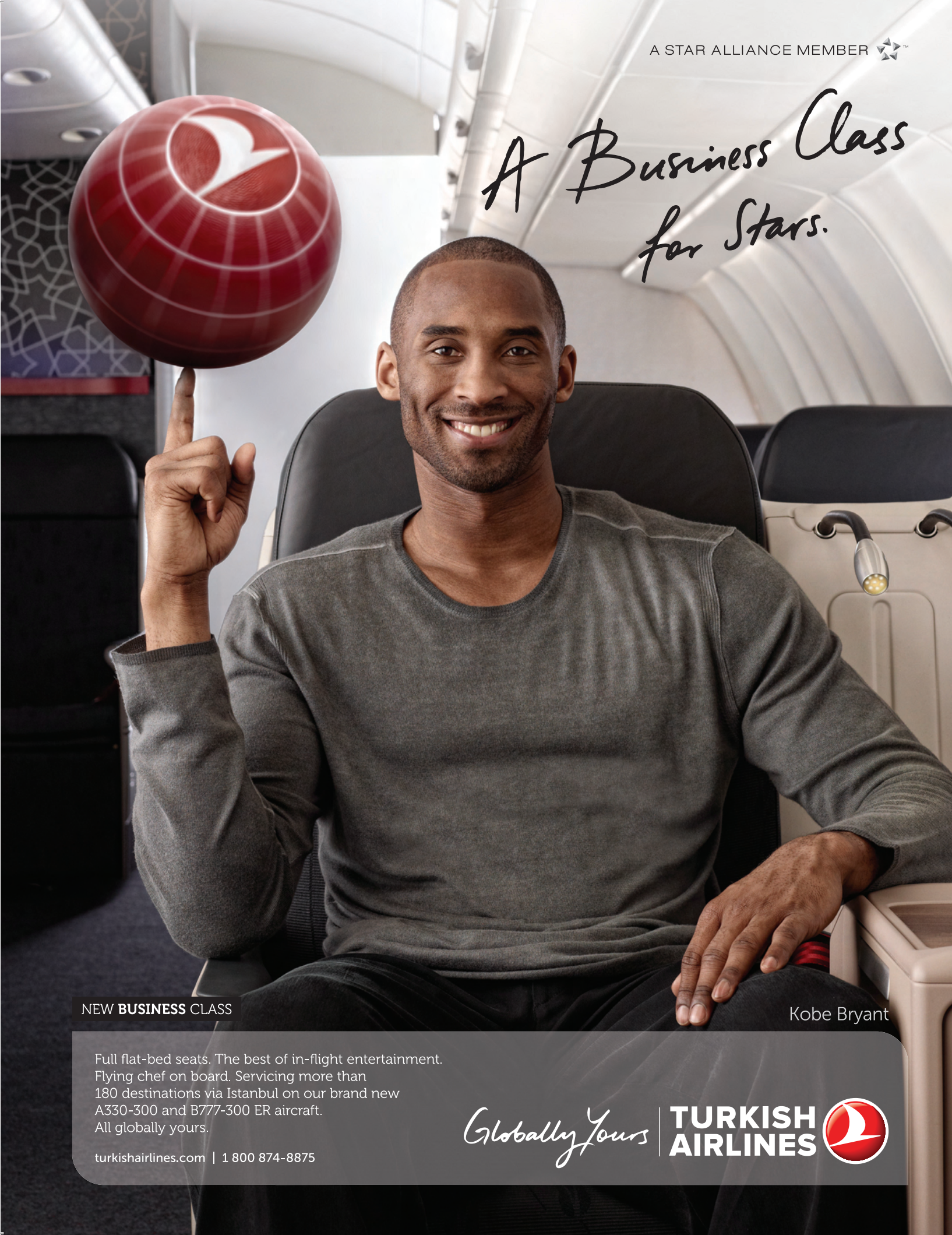
wildman.com

Wildman Harrold
Attorneys and Counselors

Complex Litigation | Business Transactions | Intellectual Property

THE ASSOCIATION OF MEDIA AND ENTERTAINMENT COUNSEL
5225 Wilshire Blvd. #417
Los Angeles, CA 90036
p: 310.432.0507
f: 310.277.1980
www.theamec.com

EXECUTIVE DIRECTOR
Serra Aladag
serra@theamec.com


A STAR ALLIANCE MEMBER
A Business Class for Stars.
NEW BUSINESS CLASS
Kobe Bryant
Full flat-bed seats. The best of in-flight entertainment.
Flying chef on board. Servicing more than
180 destinations via Istanbul on our brand new
A330-300 and B777-300 ER aircraft.
All globally yours.
turkishairlines.com | 1 800 874-8875
Globally Yours
TURKISH AIRLINES

M/E INSIGHTS

ADVANCED MEDIA

WINTER/SPRING 2011