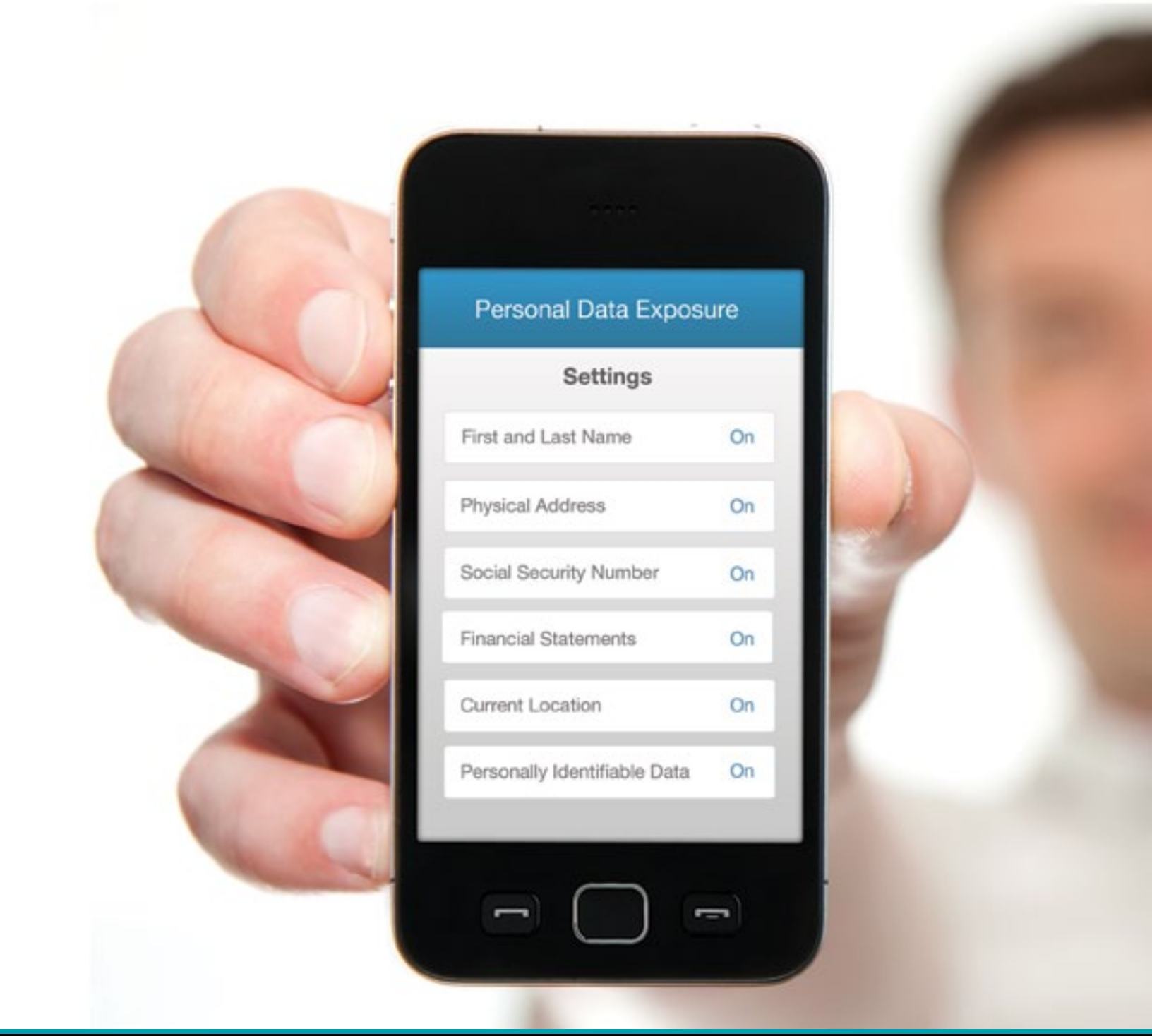
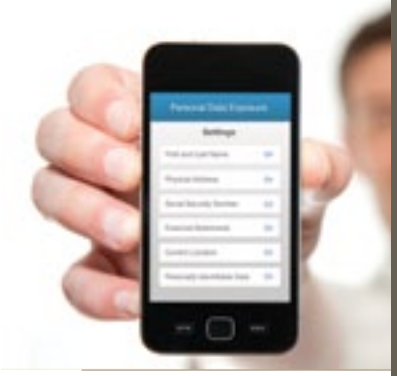
M/E INSIGHTS

ADVANCED MEDIA *WINTER/SPRING 2011*



AMEC
THE ASSOCIATION OF MEDIA & ENTERTAINMENT 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

MANAGEMENT AND ADVISORY BOARDS

EXECUTIVE DIRECTOR
Serra Aladag
serra@theamec.com

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

CONTENT

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 organizations 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 incorporate 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 producers 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

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." Bresnan 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 Bresnan'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 policies 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 you 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 Bresnan 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

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

pg. 20 to 27 pg. 28 to 31 pg. 32 to 36 pg. 37 to 39

EXECUTIVE DIRECTOR
Serra Aladag
serra@theamec.com

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