

THE JOHN MARSHALL REVIEW OF INTELLECTUAL PROPERTY LAW



SOCIAL NETWORKING AND BLOGGING: THE NEW LEGAL FRONTIER

LIISA THOMAS AND ROBERT NEWMAN

ABSTRACT

Improvements in communication technology have effectively made the world a smaller place. As businesses attempt to exploit these new technological improvements to better communicate their messages to their clients, these same improvements continue to raise new and difficult legal issues related to fair trade practices, privacy, and freedom of speech. This article identifies current legal developments related to advertising in the online world and analyzes the actions taken to resolve these new and difficult legal issues within the framework of United States federal and state law and private industry-specific self-governance.

Copyright © 2009 The John Marshall Law School



Cite as Liisa Thomas and Robert Newman, *Social Networking and Blogging: The New Legal Frontier*, 9 J. MARSHALL REV. INTELL. PROP. L. 500 (2009).

SOCIAL NETWORKING AND BLOGGING: THE NEW LEGAL FRONTIER

LIISA THOMAS AND ROBERT NEWMAN

INTRODUCTION.....	500
I. LIABILITY SHIELDS FOR THIRD-PARTY POSTINGS.....	501
A. Liability for Intellectual Property Infringements	502
1. <i>Trademark Infringement</i>	502
2. <i>Copyright Infringement</i>	504
B. Liability for Illegal Postings	506
1. <i>When the CDA Protects a Website</i>	507
2. <i>When the CDA Will Not Afford Protection</i>	509
II. LIABILITY FOR EMPLOYEE/AGENT POSTS.....	511
A. Liability for Failing to Disclose Employee Affiliation	512
B. Statements Made By Individuals Who Disclose Their Relationship	513
C. Statements Made By Individuals Who Do Not Disclose Their Relationship...	514
D. Don't Fake It.....	515
E. Liability for Investor Reliance on Employee Postings	517
III. PRIVACY OBLIGATIONS.....	517
A. CAN-SPAM and Viral Marketing with Social Media.....	518
B. Special Privacy Considerations for Children	519
1. <i>COPPA—The Starting Line</i>	520
2. <i>Growing Concern Over COPPA's Limitations—States Take Action</i>	521
3. <i>The Children's Advertising Review Unit</i>	524
CONCLUSION.....	526

SOCIAL NETWORKING AND BLOGGING: THE NEW LEGAL FRONTIER

LIISA THOMAS AND ROBERT NEWMAN *

INTRODUCTION

Blogs and social networking websites are the new marketing frontier. As consumers have adopted these forums and integrated them into their daily routines, advertisers have been quick to follow.¹ Doing so, however, is not without risk. Not only do social networking websites need to worry about liability for third-party posts,² but advertisers in those media also need to think about liability issues unique to them.³ Will advertisers be responsible for comments made by their employees on social networking sites? Will they be responsible for comments made by bloggers that they hire to discuss their products? What about the advertiser who creates its own profiles on social networking sites? Can it contract directly with other users? Will it be liable for content posts other users post on its pages? And what about social networking sites and advertisers' obligations with respect to consumers' personal information? Many courts and regulatory bodies at the federal and state level have begun to grapple with these issues.⁴ And, as they do, answers are

* This article is for informational purposes only, and should not be used as a substitute for legal advice, which turns on specific facts. For more information about the information discussed herein, please contact Liisa M. Thomas, a partner in the advertising law group at Winston & Strawn LLP. Liisa has created a unique practice focusing on interactive advertising issues, and can be reached at lmthomas@winston.com or (312) 558-6149. Robert Newman is an associate in the advertising law group, and can be reached at rnewman@winston.com or (312) 558-8125.

¹ See e.g., Google.com, Adwords, <https://adwords.google.com> (last visited Nov. 2, 2009); Knowledge@Wharton, *Who Owns You? Finding a Balance between Online Privacy and Targeted Advertising*, <http://knowledge.wharton.upenn.edu/article.cfm?articleid=1865> (last visited Nov. 2, 2009).

² See, e.g., *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.*, 545 U.S. 913, 937 (2005) (“The classic instance of inducement is by advertisement or solicitation that broadcasts a message designed to stimulate others to commit violations.”).

³ E.g., Children’s Online Privacy Protection Act of 1998, 15 U.S.C. § 6501–6506 (2006). *But see* Digital Millennium Copyright Act, 17 U.S.C. § 512 (limiting liability for service providers based on material posted online); Communications Decency Act, 47 U.S.C. § 230(c)(1) (2006) (“No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.”).

⁴ See 15 U.S.C. § 6501–6506; *Chi. Lawyers' Comm. for Civil Rights Under Law, Inc. v. Craigslist, Inc.*, 519 F.3d 666, 672 (7th Cir. 2008) (holding that craigslist, an online classified Web site, is not liable for discriminatory housing listings posted by third party users); *Doe v. MySpace, Inc.*, 528 F.3d 413, 422 (5th Cir. 2008) (holding that negligence and gross negligence claims against the social networking Web site Myspace are barred by the Communications Decency Act and affirming that the claims are also barred under Texas common law); *Carafano v. Metrosplash.com, Inc.*, 339 F.3d 1119, 1125 (9th Cir. 2003) (“[D]espite the serious and utterly deplorable consequences that occurred in this case, we conclude that Congress intended that service providers such as Matchmaker be afforded immunity from suit.”).

beginning to emerge that outline for companies how to limit liability and use social networking forums in a manner that limits risk.⁵

I. LIABILITY SHIELDS FOR THIRD-PARTY POSTINGS

Many companies create interactive websites in which third parties can communicate with each other and with the company. While this practice may allow a company to create significant buzz around its products, it can also expose the company to potential liability—in particular vicarious or contributory liability—when the user infringes on the rights of third parties or otherwise violates the law.⁶ The risk to sites that allow such postings is that they may be viewed as responsible for consumers' problematic comments or content.⁷ However, there are certain legal protections available and steps that companies can take to attempt to limit their liability for such postings. These include protections that have been viewed under common law as shielding a company from vicarious or contributory liability, as well as two statutory shields: the Digital Millennium Copyright Act ("DMCA")⁸ and the Communications Decency Act ("CDA").⁹

These different shields apply to different types of alleged infringements or legal violations. For example, while the DMCA will shield Internet service providers against certain claims of copyright infringement, the DMCA will generally not assist a company in defending a claim of trademark infringement.¹⁰ Similarly, the CDA can protect a company from certain posts containing illegal content (i.e., defamation), but, as discussed in detail below, the CDA does not apply to intellectual property infringements.¹¹

⁵ See, e.g., FED. TRADE COMM'N ET AL., HOW TO COMPLY WITH THE CHILDREN'S ONLINE PRIVACY PROTECTION RULE, available at <http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus45.pdf> [hereinafter HOW TO COMPLY].

⁶ See *Grokster*, 545 U.S. at 936–37 (“[O]ne who distributes a device with the object of promoting its use to infringe copyright, as shown by clear expression or other affirmative steps taken to foster infringement, is liable for the resulting acts of infringement by third parties.”).

⁷ See *id.*

⁸ 17 U.S.C. § 512 (2006).

⁹ 47 U.S.C. § 230 (2006).

¹⁰ 17 U.S.C. § 512(a) (providing explicit protection against claims of copyright infringement). See generally Jonathan J. Darrow & Gerald R. Ferrera, *Social Networking Websites and the DMCA: A Safe-Harbor from Copyright Infringement Liability or the Perfect Storm?*, 6 NW. J. TECH. & INTELL. PROP. 1 (2007), <http://www.law.northwestern.edu/journals/njtip/v6/n1/1/Darrow.pdf> (discussing the advantages and disadvantages of the DMCA).

¹¹ 47 U.S.C. § 230(c); see also Michael D. Marin & Christopher V. Popov, *Doe v. MySpace, Inc.: Liability for Third Party Content on Social Networking Sites*, 25 COMM. LAW. 3, 7 (2007) (summarizing the four exceptions of immunity granted by the CDA).

A. *Liability for Intellectual Property Infringements*

1. *Trademark Infringement*

If a trademark owner brought suit against a company because a user infringed the trademark owner's marks, the trademark owner would need to prove either vicarious or contributory liability.¹² There is no specific statute or regulation protecting a service provider (such as a company that hosts a social networking site) from liability for vicarious or contributory trademark infringement. To prove vicarious trademark liability in the Seventh Circuit, for example, a trademark owner must demonstrate that the website operator had an apparent or actual partnership with the user who posted the infringing material, that the company and the user had the authority to bind one another in transactions with others, or that the company and the user exercised joint control over the infringing product.¹³ To establish contributory trademark infringement, on the other hand, the trademark owner must show that the defendant either (1) intentionally induced another to infringe on its trademark rights, or (2) continued to supply a product to a third party it knows or has reason to know is engaging in trademark infringement.¹⁴ The word "product" in the second prong of this test has been broadly construed to include websites and Internet services.¹⁵ In the context of such online services, courts have generally focused their analysis on the extent of the control the service provider has over the third party's means of infringement.¹⁶

When bringing suit, most trademark owners have advanced arguments under the second theory, namely that online service providers who allow trademark infringements on their websites are contributorily liable because they continue to provide the Internet services to infringers with actual or constructive knowledge of the infringing activity.¹⁷ This argument is similar to arguments used in a line of cases examining the liability of flea market owners for trademark infringements that occur on their premises. In those cases, flea market owners who leased vending

¹² 15 U.S.C. § 1114 (2006); *see, e.g.*, *Inwood Labs., Inc. v. Ives Labs., Inc.*, 456 U.S. 844, 853–54 (1982) (“[I]f a manufacturer or distributor intentionally induces another to infringe a trademark, or if it continues to supply its product to one whom it knows or has reason to know is engaging in trademark infringement, the manufacturer or distributor is contributorily responsible for any harm done as a result of the deceit.”).

¹³ *See Hard Rock Cafe Licensing Corp. v. Concession Servs., Inc.*, 955 F.2d 1143, 1150 (7th Cir. 1992).

¹⁴ *Inwood Labs.*, 456 U.S. at 853–54; *David Berg & Co. v. Gatto Int'l Trading Co.*, 844 F.2d 306, 311 (7th Cir. 1989) (citing *Inwood Labs.*, 456 U.S. at 853–54).

¹⁵ *Perfect 10, Inc. v. Visa Int'l Serv. Ass'n*, 494 F.3d 788, 807 (9th Cir. 2007); *Lockheed Martin Corp. v. Network Solutions, Inc.*, 194 F.3d 980, 984 (9th Cir. 1999); *see, e.g.*, *Tiffany (NJ) Inc. v. eBay, Inc.*, 576 F. Supp. 2d 463, 504–06 (S.D.N.Y. 2008).

¹⁶ *Lockheed Martin*, 194 F.3d at 984; *see also Perfect 10*, 494 F.3d at 807 (indicating that contributory liability is not found where a website operator did not have “the power to remove infringing material from these websites or directly stop their distribution over the Internet.”).

¹⁷ *E.g.*, *Size, Inc. v. Network Solutions, Inc.*, 255 F. Supp. 2d 568, 572 (E.D. Va. 2003); *see also Diane Von Furstenberg Studio v. Snyder*, No. 1:06cv1356 (JCC), 2007 WL 2688184, at *11–12 (E.D. Va. Sept. 10, 2007) (“Contributory infringement occurs when the defendant either intentionally induces a third party to infringe the plaintiff's mark or supplies a product to a third party with actual or constructive knowledge that the product is being used to infringe the service mark.”) (citations omitted).

space to trademark infringers were found liable if they continued to supply that space after they had actual or constructive knowledge of the vendor's infringing activities.¹⁸ "Willful blindness," or suspecting wrongdoing and deliberately failing to investigate, is considered to be the equivalent of actual knowledge in the context of contributory trademark infringement.¹⁹

The extent to which a website would be found contributorily or vicariously liable was recently tested in the United States District Court for the Southern District of New York, where the well-known jewelry retailer Tiffany and Co. brought suit against eBay for counterfeit products sold on the eBay auction site by eBay users.²⁰ The Southern District of New York held that eBay was not contributorily or vicariously liable for sales by its users, and had no affirmative obligation to take preemptive measures such as monitoring its site for counterfeit goods.²¹ Instead, because eBay removed listings featuring counterfeit goods as soon as Tiffany notified them that a specific seller was selling an infringing product, eBay was not liable for either direct or contributory trademark infringement.²² This was the case despite the fact that eBay had "generalized" knowledge of trademark infringement on its website.²³ The court analyzed the extent of control exercised by eBay over the third party's means of infringement and concluded that "while eBay clearly possessed general knowledge as to counterfeiting on its website, such generalized knowledge is insufficient under the *Inwood* test to impose upon eBay an affirmative duty to remedy the problem."²⁴

However, the court did reiterate that contributory infringement may be found where the plaintiff can show that the defendant was "willfully blind" to the infringing activity.²⁵ For example, in the pending case of *Louis Vuitton Malletier, S.A. v. Akanoc Solutions, Inc.*, the District Court for the Northern District of California denied the defendant's motion to dismiss a claim of contributory infringement because the court concluded that a reasonable jury could find that the defendants remained willfully blind to infringing activity on websites hosted by the defendant.²⁶ The court explained that to prove contributory trademark infringement, a plaintiff must establish that the defendant "(1) intentionally induced the primary infringer to infringe, or (2) continued to supply an infringing product to an infringer with knowledge that the infringer is mislabeling the particular product supplied."²⁷ In

¹⁸ *Hard Rock Cafe*, 955 F.2d at 1145, 1150; see also *Fonovisa, Inc. v. Cherry Auction, Inc.*, 76 F.3d 259, 264–65 (9th Cir. 1996) ("*Hard Rock Cafe's* application of the *Inwood* test is sound; a swap meet can not disregard its vendors' blatant trademark infringements with impunity.>").

¹⁹ *Hard Rock Cafe*, 955 F.2d at 1149.

²⁰ *Tiffany*, 576 F. Supp. 2d at 469.

²¹ *Id.* at 527 ("[I]t is the trademark owner's burden to police its mark, and companies like eBay cannot be held liable for trademark infringement based solely on their generalized knowledge that trademark infringement might be occurring on their websites.>").

²² *Id.* at 517–18.

²³ *Id.* at 507, 511.

²⁴ *Id.* at 508.

²⁵ *Id.* at 513; e.g., *R.F.M.A.S., Inc. v. Mimi So*, 619 F. Supp. 2d 39, 84–85 (S.D.N.Y. 2009) ("[Plaintiff] can satisfy 'the 'reason to know' standard . . . by showing that the [Richemont Defendants were] willfully blind to the infringing activity.'" (quoting *Tiffany*, 576 F. Supp. 2d at 513) (second alteration in original)).

²⁶ 591 F. Supp. 2d 1098 (N.D. Cal. 2008).

²⁷ *Id.* at 1111.

order satisfy the second prong of this test, a plaintiff must prove that the defendant had knowledge *and* direct control and monitoring of the service used to infringe the plaintiff's mark.²⁸

2. Copyright Infringement

The DMCA safe harbor provides for specific relief from copyright infringement damage claims for service providers, if the service provider follows certain specific requirements.²⁹ Specifically, the DMCA limits a service provider's liability "for infringement of copyright by reason of the storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider."³⁰

In order to obtain protection under the DMCA, the service provider must first meet these thresholds: it must have either no actual knowledge of the infringement or no knowledge of facts from which it could derive such actual knowledge;³¹ it cannot receive a direct benefit from the infringement in an instance where it has the right and ability to control the content;³² and as soon as it receives proper notification from a copyright holder of an alleged infringement, it must act "expeditiously" to remove access on its site to the infringing material.³³ In addition, the service provider must register a designated agent with the copyright office, and place a notice on its site that contains the agent's name, address, telephone number, and electronic mail address.³⁴

Proper notification from the copyright holder of an alleged infringement must include the following six elements: (1) physical or electronic signature of the copyright holder or someone acting on its behalf; (2) identification of the copyrighted work allegedly infringed; (3) identification of the infringing material; (4) contact information sufficient for the service provider to contact the complaining party, such as address, telephone number, or electronic mail address; (5) a statement from the copyright holder that it has a good-faith belief that the use of the allegedly infringing material has not been authorized; and (6) a statement that the information in the notice is accurate.³⁵ In order to streamline the receipt of notification, it may be easiest to require that copyright holders or their agents complete a standardized form. If the service provider receives a notification that does not substantially comply with these six elements, it will not be deemed to have "actual knowledge" of the claim.³⁶ However, if it receives a notice that does not have a signature or

²⁸ *Id.*

²⁹ 17 U.S.C. § 512 (2006); *Corbis Corp. v Amazon.com, Inc.*, 351 F. Supp 2d 1090, 1098 (W.D. Wash. 2004).

³⁰ 17 U.S.C. § 512 (c)(1); *Io Group, Inc. v. Veoh Networks, Inc.*, 586 F. Supp. 2d 1132, 1145–46 (N.D. Cal. 2008).

³¹ 17 U.S.C. § 512(c)(1)(A)(i)–(ii).

³² *Id.* § 512(c)(1)(B).

³³ *Id.* § 512(c)(1)(A)(iii).

³⁴ *Id.* § 512(c)(2).

³⁵ *Id.* § 512(c)(3)(A).

³⁶ *Id.* § 512(c)(3)(B)(i).

statements that the notice has been sent in good faith and is accurate, the service provider must assist the copyright holder in complying with these provisions.³⁷

Upon receipt of a proper notification, the service provider must expeditiously remove the material from its site, or remove access to the material from its site.³⁸ It must then promptly notify the user who has posted the allegedly infringing material that the material has been removed.³⁹ The user may then send the service provider a counter-notification, which must meet the following four requirements: (1) it must be a written communication (i.e., a phone call to the service provider will not suffice); (2) it must include a physical or electronic signature; (3) it must identify the material in question; (4) it must include a statement that, under penalty of perjury, the material was removed either because of a mistake, or because it was misidentified; and (5) it must include the user's name, address, telephone number, and a statement that the user consents to jurisdiction in the federal district court where the service provider is located.⁴⁰ If the service provider receives a counter-notification, it must forward a copy to the copyright holder, and notify the copyright holder that it intends to re-post the material if the copyright holder does not respond in ten business days.⁴¹ If the copyright holder responds that it has filed an action seeking a court order to restrain the user's infringing activity, the service provider does not have to re-post the material.⁴² However, if no such response is received, the service provider must re-post the material within four days (i.e., between the tenth and the fourteenth day after it has sent a copy of the counter-notification to the copyright holder).⁴³

Even if a service provider has complied with these procedures, a service provider will lose the protection of the DMCA safe harbor where it (a) "has the right and ability to control [the infringing] activity" and (b) "receive[s] a financial benefit directly attributable to the infringing activity."⁴⁴ Importantly, both elements must be met in order for the safe harbor to be denied.⁴⁵ These requirements codify many of the common law principles discussed above.⁴⁶

While the DMCA would appear to provide protection to any website operator that follows the procedures described above, Viacom nevertheless recently filed suit against YouTube, operator of the well-known website that allows users to upload video content.⁴⁷ Viacom is arguing, in this still-pending case, that YouTube should not be afforded DMCA protection because YouTube knows, or should know, that its website contains infringing materials inasmuch as YouTube has the right and ability to control the content on the site, and receives a direct financial benefit from the

³⁷ *Id.* § 512(c)(3)(B)(ii).

³⁸ *Id.* § 512(c)(1)(A)(iii).

³⁹ *Id.* § 512(g)(2)(A).

⁴⁰ *Id.* § 512(g)(3).

⁴¹ *Id.* § 512(g)(2)(B).

⁴² *Id.* § 512(g)(2)(C).

⁴³ *Id.*

⁴⁴ *Id.* § 512(c)(1)(B).

⁴⁵ *Id.*; *Io Group, Inc. v. Veoh Networks, Inc.*, 586 F. Supp. 2d 1132, 1150 (N.D. Cal. 2008); *Corbis Corp. v. Amazon.com, Inc.*, 351 F. Supp. 2d 1090, 1109 (W.D. Wash. 2004).

⁴⁶ *Veoh Networks*, 586 F. Supp. 2d at 1150 ("These requirements grew out of the common law standard for vicarious liability, and the Ninth Circuit has indicated that these elements under the DMCA are to be interpreted consistently with common law." (citing *Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102, 1117 (9th Cir. 2007))).

⁴⁷ *Viacom Int'l Inc. v. YouTube Inc.*, 253 F.R.D. 256 (S.D.N.Y. 2008).

content.⁴⁸ This case is still pending before the District Court for the Southern District of New York, and its outcome may alter the analysis outlined above.

However, a recent California District Court case may provide some guidance. In *Io Group, Inc. v. Veoh Networks, Inc.*, the court found that Veoh Networks, a company that provides a video-sharing service similar to YouTube, was not liable for copyright infringement for material uploaded to its website because Veoh Networks complied with the takedown and other procedural provisions described in the DMCA.⁴⁹ The court held that even though infringing material was posted to the website, Veoh qualified for “safe harbor” under the DMCA.⁵⁰ The court reached this conclusion in part because it found that all video files are uploaded to Veoh through an automated process that is initiated entirely by users.⁵¹ In addition, the court found that Veoh has a strong DMCA policy in place and takes “active steps to limit incidents of infringement on its website.”⁵² Consequently, Veoh was found to qualify for the DMCA safe harbors and prevailed on its motion for summary judgment.⁵³

B. Liability for Illegal Postings

Section 230 of the Communications Decency Act of 1996⁵⁴ (“CDA”) has been interpreted by courts to protect blogs and social networking websites when defamatory, obscene, pornographic, or other offensive or illegal material is posted on such site by a third party.⁵⁵ Specifically, section (c)(1) of the CDA provides that “[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another content provider.”⁵⁶ The CDA defines “interactive computer service” as “any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet.”⁵⁷ The Act also defines “information content provider” as “any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service.”⁵⁸

A company sued for the content posted by its website users should enjoy immunity under the CDA if: (1) it is a provider or user of an interactive computer service; (2) it did not act as an information content provider with respect to the information that was posted; and (3) the asserted claims treat the defendant as a

⁴⁸ *See id.*

⁴⁹ 586 F. Supp. 2d at 1155.

⁵⁰ *Id.* at 1154.

⁵¹ *Id.* at 1148 (“Veoh does not itself actively participate or supervise the uploading of files. Nor does it preview or select the files before the upload is completed. Instead, video files are uploaded through an automated process which is initiated entirely at the volition of Veoh’s users.”).

⁵² *Id.* at 1155.

⁵³ *Id.*

⁵⁴ 47 U.S.C. § 230 (2006).

⁵⁵ *E.g.*, *Doe v. MySpace, Inc.*, 474 F. Supp. 2d 843, 847–48 (W.D. Tex. 2007), *aff’d*, 528 F.3d 413 (5th Cir. 2008).

⁵⁶ 47 U.S.C. § 230(c)(1).

⁵⁷ *Id.* § 230(f)(2).

⁵⁸ *Id.* § 230(f)(3).

publisher or speaker of information originating from a third party.⁵⁹ Courts traditionally treat “§ 230(c) immunity as quite robust, adopting a relatively expansive view of ‘interactive computer service’ and a relatively restrictive definition of ‘information content provider.’”⁶⁰ For example, Amazon.com has been found to be the provider of an “interactive computer service” because it enables users to post comments about books, and was thus shielded under the CDA.⁶¹ Likewise, Matchmaker.com—a website dating service permitting members of the service to search a database of profiles posted by other members—was found to be the provider of an interactive computer service because it enabled thousands of its members to access and use a searchable database maintained on its computer servers.⁶²

1. *When the CDA Protects a Website*

The CDA “creates a federal immunity to any cause of action that would make service providers liable for information originating with a third-party user of the service.”⁶³ This immunity has been broadly construed by the courts.⁶⁴ The types of claims for which CDA has been used as a shield are numerous and diverse. For example, Craigslist.com used the CDA when it was sued for failure to screen for the sale of a handgun on its site which was later used in the commission of an assault against the plaintiff.⁶⁵ Craigslist.com also used the CDA in the Seventh Circuit as a

⁵⁹ See *MCW, Inc. v. Badbusinessbureau.com, L.L.C.*, No. Civ.A.3:02-CV-2727-G, 2004 WL 833595, at *8 (N.D. Tex. Apr. 19, 2004).

⁶⁰ *Carafano v. Metrosplash.com, Inc.*, 339 F.3d 1119, 1123 (9th Cir. 2003).

⁶¹ *Schneider v. Amazon.com, Inc.*, 31 P.3d 37, 40 (Wash. Ct. App. 2001).

⁶² *Carafano v. Metrosplash.com*, 207 F. Supp. 2d 1055, 1065–66 (C.D. Cal. 2002), *aff’d on other grounds*, 339 F.3d 1119 (9th Cir. 2003).

⁶³ *Zeran v. America Online, Inc.*, 129 F.3d 327, 330 (4th Cir. 1997); see also *Carafano*, 339 F.3d at 1125 (applying CDA immunity to defendant “even assuming Matchmaker could be considered an interactive content provider”); *United States v. Jackson*, 208 F.3d 633, 637 (7th Cir. 2000) (noting that service providers are “merely conduits” for information); *Atl. Recording Corp. v. Project Playlist, Inc.*, 603 F. Supp. 2d 690, 700–01 (S.D.N.Y. 2009) (finding Defendant was not an “information content provider” under the CDA because defendant neither created nor developed the relevant information on the website); *Doe v. Friendfinder Network, Inc.*, 540 F. Supp. 2d 288, 293 (D.N.H. 2008) (applying CDA immunity where defendant neither created nor developed the relevant content); *Global Royalties, Ltd. v. Xcentric Ventures, LLC*, 544 F. Supp. 2d 929, 932 (D. Ariz. 2008) (“[T]he CDA is a complete bar to a suit against a website operator for its ‘exercise of a publisher’s traditional editorial functions’” (quoting *Zeran*, 129 F.3d at 330)); *Nemet Chevrolet, Ltd. v. Consumeraffairs.com, Inc.*, 564 F. Supp. 2d 544, 555 (E.D. Va. 2008) (applying CDA immunity where “Defendant was merely a[n] interactive computer service”); *Blumenthal v. Drudge*, 992 F. Supp. 44, 52 (D.D.C. 1998) (indicating that service providers are unlike other information providers because they provide an interactive medium, and thus Congress provided special immunity for providers that police their content); *Doe v. America Online*, 718 So. 2d 385, 389 (Fla. Dist. Ct. App. 1998) (holding that America Online could not be found liable as a distributor for obscene material posted on the Internet); *Does v. Franco Prods.*, No. 99 C 7885, 2000 WL 816779, *4 (N.D. Ill. June 22, 2000) (“[The CDA] creates a federal immunity to any cause of action that would make service providers liable for information originating with a third-party user of the service.” (quoting *Zeran*, 129 F.3d at 330)).

⁶⁴ See, e.g., *Gibson v. Craigslist, Inc.*, No. 08 Civ. 7735(RMB), 2009 WL 1704355, at *3 (S.D.N.Y. June 15, 2009) (“Courts across the country have repeatedly held that the CDA’s grant of immunity should be construed broadly.” (quoting *Atl. Recording Corp.*, 603 F. Supp. 2d at 699)).

⁶⁵ *Id.*

shield against liability arising under the Fair Housing Act,⁶⁶ MySpace has used the CDA as a defense against liability for personal injuries stemming from content posted to its site (where a young girl was victimized by an online predator),⁶⁷ and Yahoo! has used the CDA as a shield against claims for negligence, infliction of emotional distress, invasion of privacy, and civil conspiracy where parents brought suit against the company for allowing a user to host an illegal child pornography e-group.⁶⁸

Google, too, has used the CDA to its advantage.⁶⁹ The United States District Court for the Northern District of California recently dismissed a lawsuit brought against Google based on fraudulent advertisements appearing in its AdWords program.⁷⁰ In reaching its decision, the court found that the fact that Google elicits the posted content for profit does not undermine Google's immunity under the CDA.⁷¹

In seeking protection under the CDA, companies typically take some affirmative steps, although none are technically required. For example, companies post rules clearly stating that postings that violate third-party rights are not allowed, that they have the right to delete any posting which violates its stated rules, and that they have the right to deactivate a registered user who violates the rules.⁷² Users should be required to read and accept the rules before posting content, and the rules should be easy to find on the website after the user has initially accepted them.⁷³ Companies will also need to analyze the extent to which they are viewed merely as a passive publisher of the information, or where they may be viewed as more actively involved in the creation of the information. Where a company is an active creator, it is unlikely to be afforded CDA immunity.⁷⁴

⁶⁶ See Chi. Lawyers' Comm. for Civil Rights Under Law, Inc. v. Craigslist, Inc., 519 F.3d 666, 669, 672 (7th Cir. 2008).

⁶⁷ See Doe v. MySpace, Inc., 474 F. Supp. 2d 843, 849–50 (W.D. Tex. 2007), *aff'd*, 528 F.3d 413 (5th Cir. 2008).

⁶⁸ See Doe v. Bates, No. 5:05-CV-91-DF-CMC, 2006 WL 3813758, at *3–5 (E.D. Tex. Dec. 27, 2006).

⁶⁹ See Goddard v. Google, Inc., No. C 08-2738 JF (PVT), 2008 WL 5245490, at *7 (N.D. Cal. Dec. 17, 2008) (granting Google's motion to dismiss because plaintiff failed to allege that Google was the "information content provider" for the relevant content).

⁷⁰ *Id.*

⁷¹ *Id.* at *3 ("[T]he fact that a website elicits online content for profit is immaterial; the only relevant inquiry is whether the interactive service provider 'creates' or 'develops' that content." (citing Blumenthal v. Drudge, 992 F. Supp. 44, 52 (D.D.C. 1998))).

⁷² *E.g.*, Facebook, Statement of Rights and Responsibilities, ¶ 5, <http://www.facebook.com/terms.php?ref=pf> (last visited Nov. 7, 2009).

1. You will not post content or take any action on Facebook that infringes or violates someone else's rights or otherwise violates the law.
2. We can remove any content or information you post on Facebook if we believe that it violates this Statement. . . .
-
5. If you repeatedly infringe other people's intellectual property rights, we will disable your account when appropriate.

Id.

⁷³ See *id.*

⁷⁴ See 47 U.S.C. § 230(c)(1) (2006) (offering immunity only when the information content provider is not the service provider itself); *id.* § 230(f)(3) (defining information content provider as "any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service"); *Goddard*,

2. When the CDA Will Not Afford Protection

The owner of a social networking website can be both a service provider, protected by the CDA, and a content provider, not protected by the CDA.⁷⁵ Simply put, if the website operator creates, or is responsible, in whole or in part, for creating or developing the content, the website is also a content provider.⁷⁶ Where a company is an active creator or developer of content, in whole or in part, it is unlikely to be afforded CDA immunity.⁷⁷ For example, in *Fair Housing Council of San Fernando Valley v. Roommates.com, LLC*, the United States Court of Appeals for the Ninth Circuit considered a case brought by a fair housing council against an online roommate matching website for violation of the Fair Housing Act and state laws.⁷⁸ The court held that when Roommates.com asked questions that members were required to answer in order to create member profiles and organized that information based on the member's answers, Roommates.com was not protected by the CDA because it was serving as an "information content provider."⁷⁹

The court reasoned that because the CDA defines a content provider as "any person or entity that is responsible, *in whole or in part*, for the creation or development of information provided through the Internet," if Roommates.com is partially responsible for the creation or development of information, it is considered a content provider and is not entitled to CDA immunity.⁸⁰ However, the court found that Roommates.com was not an information content provider where it merely requested "additional information" and left a blank text box in which end users could enter information.⁸¹ This case was reheard by the Ninth Circuit *en banc*, and the court concluded that "[b]y requiring subscribers to provide the information as a condition of accessing its service, and by providing a limited set of pre-populated answers, Roommate becomes much more than a passive transmitter of information provided by others; it becomes the developer, at least in part, of that information."⁸²

Merely asking questions of visitors to social networking sites, however, is unlikely to result in the website being considered a content provider. For example, in *Doe v. MySpace, Inc.*, the United States District Court for the Eastern District of Texas distinguished the Ninth Circuit's decision in *Roommates.com, LLC*, on the grounds that because users of MySpace.com are not required to provide any additional information in their profiles, the fact that MySpace asks certain questions does not convert MySpace into a content provider.⁸³

2008 WL 5245490, at *3 ("[W]here a third party 'creates' the allegedly unlawful content, an interactive computer service provider may be liable for its publication if it 'helps to develop [the] unlawful content,' meaning that it 'contributes materially to the alleged illegality of the conduct.'" (quoting *Fair Hous. Council of San Fernando Valley v. Roommates.Com, LLC*, 521 F.3d 1157, 1168 (9th Cir. 2008) (en banc) (alteration in original))).

⁷⁵ *Roommates.com*, 521 F.3d at 1162.

⁷⁶ *Id.*

⁷⁷ *See id.* at 1168; *Goddard*, 2008 WL 5245490, at *3.

⁷⁸ 489 F.3d 921, 924 (9th Cir. 2007), *rev'd en banc*, 521 F.3d 1157 (9th Cir. 2008).

⁷⁹ *Id.* at 926.

⁸⁰ *Id.* at 925 (quoting 47 U.S.C. § 230(f)(3) (2006)).

⁸¹ *Id.* at 929.

⁸² *Roommates.com*, 521 F.3d at 1166.

⁸³ 629 F. Supp. 2d 663, 665 (E.D. Tex. 2009).

CDA immunity has also been found not to apply where the website actively and specifically encourages development of illegal content. For example, in *FTC v. Accusearch Inc.*, the United States Court of Appeals for the Tenth Circuit considered a case in which the website commissioned third-party researchers to provide personal information about individuals following the request of a customer.⁸⁴ The court held that the word “responsible” in the definition of “content provider” in the CDA necessarily meant that Accusearch Inc. was a “content provider” because it solicited requests for the information and then paid researchers to obtain it.⁸⁵

Courts have in general interpreted the CDA not to grant immunity from liability for claims that allege violations of traditional intellectual property rights, such as claims for trademark or copyright infringement, inasmuch as the Act specifically states that it does not “limit or expand any law pertaining to intellectual property.”⁸⁶ For example, in *Almeidia v. Amazon.com, Inc.*, the United States Court of Appeals for the Eleventh Circuit noted that while few federal courts “have considered the effect of § 230(e)(2) on the CDA’s grant of immunity,” federal district courts “have held that § 230(e)(2) unambiguously precludes applying the CDA to immunize interactive service providers from trademark claims.”⁸⁷ By its terms, the CDA does not apply to “any law pertaining to intellectual property.”⁸⁸ Some courts have interpreted this to apply to laws pertaining to “federal intellectual property,”⁸⁹ while other have disagreed, and have indicated that the CDA does not provide immunity for either federal *or* state intellectual property claims.⁹⁰ While the CDA is normally viewed as protecting a company against illegal postings by third parties, it is not clear that immunity exists for claims of false advertising.⁹¹

Similarly, the CDA is unlikely to provide protection for a company against claims of breach of contract or promissory estoppel. For example, in *Barnes v. Yahoo! Inc.*, the Ninth Circuit held that while the CDA bars tort claims based on a site’s failure to remove illegal content posted by a third party, a defendant who has promised to remove such content and fails to do so may be found liable for breach of contract.⁹²

⁸⁴ 570 F.3d 1187, 1191 (10th Cir. 2009).

⁸⁵ *Id.* at 1199.

⁸⁶ 47 U.S.C. § 230(e)(2) (2006).

⁸⁷ 456 F.3d 1316, 1322 (11th Cir. 2006); *see also Novak v. Overture Servs., Inc.*, 309 F. Supp. 2d 446, 453 (E.D.N.Y. 2004) (declining to find that plaintiff’s claim sounded in trademark and that immunity was thus not available to defendants).

⁸⁸ 47 U.S.C. § 230(e)(2).

⁸⁹ *See Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102, 1119 (9th Cir. 2007) (“In the absence of a definition from Congress, we construe the term ‘intellectual property’ to mean ‘federal intellectual property.’”).

⁹⁰ *See Atl. Recording Corp. v. Project Playlist, Inc.*, 603 F. Supp. 2d 690, 704 (S.D.N.Y. 2009) (citing *Doe v. Friendfinder Network, Inc.*, 540 F. Supp. 2d 288, 302 (D.N.H. 2008)).

⁹¹ *Compare Perfect 10*, 488 F.3d at 1119, 1119 n.5 (concluding that state intellectual property claims are eligible for CDA immunity because “[a]s a practical matter, inclusion of rights protected by state law within the ‘intellectual property’ exemption would fatally undermine the broad grant of immunity provided by the CDA.”), *with Atl. Recording Corp.*, 603 F. Supp. 2d at 704 (“I conclude, as a matter of law, that *Section 230(c)(1)* does not provide immunity for either federal or state intellectual property claims.” (citing *Friendfinder*, 540 F. Supp. 2d at 302)).

⁹² 570 F.3d 1096, 1109 (9th Cir. 2009).

II. LIABILITY FOR EMPLOYEE/AGENT POSTS

The protections discussed above *do not apply* to content posted by the company, its own employees, or third-party contractors that the company has engaged to post content, nor to other content that the company is viewed as taking part in creating.⁹³ Companies are thus understandably concerned about the extent of their liability for such statements, and steps they can take to limit liability. Case law in this area is still developing, and there are not yet clear answers regarding a company's liability for such activities.

As an initial matter, companies must keep in mind that the material they post (or engage others to post) on their websites, on Twitter and Facebook, or the videos they upload to YouTube, will be considered advertising.⁹⁴ As such, the posts and materials must comply with all applicable laws and express and implied claims must be truthful and accurate.⁹⁵ All of these activities, and others, might result in potential risk for a company whose employers, agents, or other third parties are engaging in online communications on its behalf.⁹⁶ For example, someone who believes he/she has been injured by an individual's claims might bring suit against the employer, rather than (or in addition to) the employee.⁹⁷

Even in the absence of extensive or clear case law or statutory direction, there is some precedent and direction for companies to consider for managing risks such as the need to disclose company affiliation, corporate liability if an employee or agent engages in illegal activity, and liability if the individual discloses confidential information or information that might influence the investors of a publicly traded company.⁹⁸ In general terms, companies should attempt to limit their exposure by ensuring that they are not acting secretly in their social media activities. For example, companies should disclose their connections to a poster when the company hired the person giving an opinion, the company provided a free product to the

⁹³ 47 U.S.C. § 230(c)(1) (“No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information *provided by another* information content provider.”) (emphasis added).

⁹⁴ See, e.g., *In re Cardo Systems, National Advertising Division Case No. 4934* (2008).

⁹⁵ See, e.g., *id.*

⁹⁶ See David Kesmodel & John R. Wilke, *Whole Foods CEO Hid on Message Board*, SMARTMONEY, July 12, 2007, <http://www.smartmoney.com/breakingnews/smw/?story=20070712105705> (describing how John Mackey, the CEO of Whole Foods Market, became an example of an employee whose personal posts affected his company). In an FTC investigation of the merger between Whole Foods and its competitor Wild Oats Market, the FTC discovered that Mackey had been posting on Yahoo!'s stock market forum for years, making disparaging remarks about Wild Oats Market. *Id.* Mackey commented that the posts were never intended to be identified with him, and were simply made for entertainment purposes. *Id.* While Mackey's posts did not result ultimately in legal liability for his company, his argument that the posts should not be associated with his company were widely dismissed by commenters. See, e.g., Margo Reder, *CEO Postings – Leveraging the Internet's Communications Potential While Managing the Message to Maintain Corporate Governance Interests in Information Security, Reputation, and Compliance*, 7 DEPAUL BUS. & COM. L.J. 179, 187–89 (2009) (describing Mr. Mackey's duties as an agent of Whole Foods).

⁹⁷ See, e.g., Complaint at 5 ¶ 16, *Ward v. Cisco*, No. 4:08-cv-04022-JLH (W.D. Ark. Mar. 13, 2008) (alleging the company knew and encouraged posting of the employee's statements).

⁹⁸ See, e.g., AM. BAR FOUND., MODEL BUSINESS CORPORATION ACT § 8.56(a)(2)(B)(iii) (2002) (preventing indemnification of a corporate officer for only “an *intentional* violation of criminal law” (emphasis added)).

person giving an opinion, the company is otherwise compensating the person giving the opinion with premiums such as free points or sweepstakes entries, the company is asking its employees to “tell their friends” or otherwise take action, or employees are acting in furtherance of the company’s business and within the scope of their employment. Creating internal policies that take into account the practical realities of social networking tools may help limit a company’s risk.

A. Liability for Failing to Disclose Employee Affiliation

Under Federal Trade Commission (“FTC”) guidance, employees or other individuals who make statements in support of their companies (or companies with whom they have an affiliation and have been asked to engage in blogging) on third-party blogs will need to disclose their affiliation with their companies. The FTC enforces this guidance under its authority through the Deceptive Trade Practices Act (section 5 of the FTC Act),⁹⁹ which prohibits companies from engaging in any practice that is “deceptive” or “unfair.”¹⁰⁰ It is not always clear what the FTC will consider a deceptive or unfair practice, and for this reason, the FTC has promulgated several guidelines to give companies direction about what acts the FTC will pursue. One such guideline is the recently updated FTC Guides Concerning the Use of Endorsements and Testimonials in Advertising (“Endorsement Guides”).¹⁰¹ The Endorsement Guides were last updated in 1980 and the revised version of the Endorsement Guides went into effect on December 1, 2009.¹⁰² Under the Endorsement Guides, a person making a statement promoting the products or services of a company must—if there is a “material connection between the endorser and the seller of the advertised product” which might “affect the weight or credibility of the endorsement”—fully disclose that connection.¹⁰³ Because knowledge by readers of the posting about the person’s employment would likely impact how they viewed that posting, the relationship, according to the FTC, must be disclosed.¹⁰⁴ This disclosure requirement holds true whether the employee posts to his or her own page, or posts to the site of a third party.¹⁰⁵

In the online world, this would mean that if someone is posting about a company’s products and those posts appear to encourage others to purchase the company’s products—for example by touting the products’ benefits—and there is a material connection between the individual and the company, then the individual needs to disclose his connection to the company. Indeed, in the recently adopted amended Endorsement Guides, the FTC provides as an example a situation where an employee posts a message on a third-party message board, which message promotes

⁹⁹ 15 U.S.C. §§ 41–58 (2006). Civil penalties for violations are set on a case-by-case basis by the FTC, and range anywhere from a few thousand dollars to millions of dollars, depending in part on the severity of the violation and the financial resources of the company. *See id.* § 45(l).

¹⁰⁰ *Id.* § 45(a)(1).

¹⁰¹ Guides Concerning Use of Endorsements and Testimonials in Advertising, 16 C.F.R. pt. 255 (2009).

¹⁰² *Id.*

¹⁰³ *Id.* § 255.5.

¹⁰⁴ *See id.*

¹⁰⁵ *See id.*

the employer's product or services.¹⁰⁶ According to the FTC, the relationship must be disclosed.¹⁰⁷

For purposes of the FTC Endorsement Guidelines, the issue to examine is whether the postings appear to be comments that encourage the purchase of the company's products or services. Internal policies can thus be helpful in outlining to employees or other individuals who have been asked to post on the company's behalf, when and how they should discuss the company or its products or services in online forums.

B. Statements Made by Individuals Who Disclose Their Relationship

If employees or others acting for or on behalf of the company disclose their affiliation with their company for purposes of the FTC Endorsement Guidelines, there is a strong risk that statements they make will be considered as coming from or being made on behalf of the company. For example, if an employee or agent of the company discloses on a retailer's website that a food product is healthy and tastes delicious, and discloses that he or she has been hired by the company to discuss his or her experience with the product, consumers will likely believe that the individual's statements are sponsored or endorsed by the company. If the statement is false or unsubstantiated, the company could be at risk for false advertising liability.¹⁰⁸ With respect to employees, whether or not the statements made by the employee—who clearly discloses his or her relationship to the company, or whose relationship is otherwise generally well known—is attributed to his or her employer is governed by the doctrine of *respondeat superior*.¹⁰⁹

The requirements for establishing a claim vary from state to state, but in general an employee is found to be acting in the scope of his or her employment if the act is: (1) within the employee's general authority; (2) in furtherance of the employer's business; and (3) in furtherance of the objective for which the employee was employed.¹¹⁰ For example, in *Texam Oil Corp. v. D.D. Poynor*, the court refused to dismiss an action against a company whose employee made allegedly slanderous remarks.¹¹¹ The court found persuasive the fact that the slanderous remarks at issue were made by the then-director of the corporation while discussing business.¹¹² Because the statements were made while he was discussing business, they were clearly, according to the court, made within the employee's scope of employment.¹¹³

In another case, a radio host's employer was held liable for the defamatory

¹⁰⁶ *Id.*

¹⁰⁷ *Id.* at 72,394.

¹⁰⁸ See 15 U.S.C. § 45(a), 52 (2006).

¹⁰⁹ See, e.g., *State by Sannaus v. Mecca Enters., Inc.*, 262 N.W. 2d 152, 153, 155 (Minn. 1978).

¹¹⁰ See, e.g., *Rodriguez v. Sarabyn*, 129 F.3d 760, 767 (5th Cir. 1997) (articulating the Texas standard for *respondeat superior*); see also *McPherson v. Red Robin Int'l, Inc.*, No. 8:04CV51, 2005 WL 2671033, at *6 (D. Neb. Oct. 19, 2005) (articulating the Nebraska standard for *respondeat superior*).

¹¹¹ 436 S.W.2d 129, 129–30 (Tex. 1968) (per curiam).

¹¹² *Id.* at 129.

¹¹³ *Id.*

statements made by one of its radio personalities during the radio host's show.¹¹⁴ That an employee makes a statement on an online blog site, even a non-employer site, is not likely to change the *respondeat superior* analysis. An employer may still potentially be liable for claims arising from such statements if the employee's statements are viewed to be within his or her scope of employment—for example if he or she is discussing products of the company, work he or she does at the company, or is making an analysis that falls within the scope of the expertise for which he or she is employed by the company.¹¹⁵

C. Statements Made by Individuals Who Do Not Disclose Their Relationship

Even if an individual does not disclose his or her affiliation with the company, for example, if the person is not endorsing or promoting the company or its products or services or is blogging anonymously, there are still risks to the company, especially if the person is an employee or otherwise engaged to blog by the company, and is commenting on the products or services of third parties.¹¹⁶ Statements might include, for example, a representation that a celebrity uses a particular product, or that the products of another company are inferior. Even if the person is not acting with the company's express authorization, it is possible the company may be liable.¹¹⁷

The recently revised Endorsement Guides have clarified that advertisers and manufacturers as well as endorsers are subject to liability for false or unsubstantiated statements made through endorsements by endorsers.¹¹⁸ The Endorsement Guides provide that if there is a material connection between the endorser and the seller of the advertised product which might affect the weight or credibility of the endorsement, such connection must be fully disclosed.¹¹⁹ The Endorsement Guides provide several examples of situations which would require disclosure of material connections in various contexts.¹²⁰ In one example, a well known blogger blogs about a company's product on his own blog site after receiving a free trial of the product from the company.¹²¹ In such case, the FTC indicated that the blogger should clearly and conspicuously disclose that he received the product for free.¹²² The FTC has not designated any particular format in which the disclosure of a material connection must be made, only that such a disclosure must be "clear and conspicuous."¹²³

In 2008, Cisco Systems was sued because of allegedly false and defamatory

¹¹⁴ *Embrey v. Holly*, 442 A.2d 966, 968, 973 (Md. 1981).

¹¹⁵ *See, e.g., Rodriguez v. Sarabyn*, 129 F.3d 760, 767 (5th Cir. 1997).

¹¹⁶ *See id.*

¹¹⁷ *See id.* ("An employer is liable for the foreseeable intentional and malicious acts of its employees done within the scope of employment, even if not authorized.") (citations omitted).

¹¹⁸ Guides Concerning the Use of Endorsements and Testimonials in Advertising, 73 Fed. Reg. 72,374, 72,377 (proposed Nov. 28, 2008) (to be codified at 16 C.F.R. pt. 255).

¹¹⁹ Guides Concerning Use of Endorsements and Testimonials in Advertising, 16 C.F.R. § 255.5 (2009).

¹²⁰ *See* Guides Concerning Use of Endorsements and Testimonials in Advertising, 16 C.F.R. pt. 255 (2009).

¹²¹ 73 Fed. Reg. 72,374, 72,395 (proposed Nov. 28, 2008) (to be codified at 16 C.F.R. pt. 255).

¹²² *Id.*

¹²³ *Id.*

statements made anonymously in an online blog by one of its employees.¹²⁴ The case is currently pending, and it remains to be established whether Cisco authorized the employee to make the allegedly infringing statements in his blog. Even if the statements were not specifically authorized by Cisco, the plaintiff in this case is arguing that Cisco should nevertheless be liable, as the employee made the statements within the scope of his employment.¹²⁵ If the court accepts this argument, and if the statements are indeed found to be infringing, then it is possible that Cisco will have financial liability to the plaintiff for its employee's statements.

Similar problems could arise if third parties who often work with or on behalf of the company make statements about the company or its products and services. For example, in an offline case, several of Amway's distributors (not employees, but individuals who often engaged in activities on Amway's behalf, such as distributing its products) left voice messages, which included false claims about Amway's competitor, Procter & Gamble ("P&G") (namely, that P&G's president was associated with the Church of Satan).¹²⁶ At issue in the case, among other things, was whether the statements, which were made by non-employees, were actually made by or on behalf of the company such that the company could be sued for its distributors' messages.¹²⁷ The Tenth Circuit found that there was insufficient evidence in that case to show that the distributors were acting either at the express direction of Amway, or with Amway's implied authorization.¹²⁸ However, to the extent that a plaintiff is able to establish one of the following, then the company may be found responsible for the posts of the agent: (1) the company's agent was acting under express instructions (express actual authority); (2) the agent was committing acts which were incidental to or necessary to realize the company's objectives (implied actual authority); or (3) the agent led a third party to believe he or she had authority from the employer to make such statements (apparent authority).¹²⁹

D. Don't Fake It

State attorneys general and the FTC are closely monitoring blogs and social networking websites for advertising claims and are bringing actions against companies who engage individuals to post material that gives the false impression that the employee is a satisfied customer.¹³⁰ For example, New York Attorney General Andrew Cuomo recently brought an action against Lifestyle Lift for using its employees to pose as satisfied customers and post reviews on a number of websites.¹³¹

¹²⁴ Plaintiff's First Amended Complaint at 9, *Ward v. Cisco Sys., Inc.*, No. 08-cv-04022-JLH (W.D. Ark. June 2, 2009).

¹²⁵ *Id.* at 10.

¹²⁶ *Procter & Gamble Co. v. Haugen*, 222 F.3d 1262, 1268 (10th Cir. 2000).

¹²⁷ *Id.* at 1278.

¹²⁸ *Id.*

¹²⁹ *Id.* (citing *Zions First Nat'l Bank v. Clark Clinic Corp.*, 762 P.2d 1090, 1094–95 (Utah 1988)).

¹³⁰ Jennifer Peltz, *Phony online reviews draw FTC scrutiny*, ORLANDO SENTINEL, July 31, 2009, at A22, available at 2009 WLNR 14801458.

¹³¹ Press Release, Office of the Attorney Gen. of N.Y., Attorney Gen. Cuomo Secures Settlement with Plastic Surgery Franchise that Flooded Internet with False Positive Reviews (July 14, 2009)

The company ultimately settled the complaint for \$300,000.¹³² In June 2009, Andrew Cuomo also reached settlement agreements with seven New York electronics companies for, among other deceptive business practices, obtaining fake consumer testimonials through pay-per-click based websites with content provided by the website owners.¹³³ The companies were required to pay approximately \$765,000 in restitution.¹³⁴

There have also been recent administrative actions against fake blogs. For example, on August 11, 2009, the Electronic Retailing Self-Regulation Program (“ERSP”) issued an opinion following a competitor’s challenge of Urban Nutrition’s website.¹³⁵ The website claimed to be an unbiased resource for consumers regarding weight loss and diet products, but the ERSP found that Urban Nutrition owned several of the weight loss and diet websites it was reviewing.¹³⁶ The FTC Endorsement Guides state the following:

When there exists a connection between the endorser and the seller of the advertised product which might materially affect the weight or credibility of the endorsement . . . such connection must be fully disclosed. . . . [W]hen the endorser is neither represented in the advertisement as an expert nor is known to a significant portion of the viewing public, then the advertiser should clearly and conspicuously disclose either the payment or promise of compensation prior to and in exchange for the endorsement¹³⁷

Consequently, ERSP recommended that Urban Nutrition include additional disclosures and make several modifications in future advertising and clearly and conspicuously disclose the nature of the relationship between Urban Nutrition and the products being reviewed to consumers immediately upon visiting the site.¹³⁸

Failure to disclose relationships between a company and its endorsers can also result in public relations headaches for the company. For example, in 2006, Sony Computer Entertainment America launched an online viral advertising campaign known as “All I Want for Christmas is a PSP.”¹³⁹ The website contained video and blogs that were supposedly created by two teenagers who were lobbying their parents, but were actually created by Sony’s advertising company as part of an

(on file with The John Marshall Review of Intellectual Property Law), *available at* http://www.oag.state.ny.us/media_center/2009/july/july14b_09.html.

¹³² *Id.*

¹³³ Press Release, Office of the Attorney Gen. of N.Y., Attorney Gen. Cuomo Secures Agreements with Seven Elecs. Cos. in N.Y. for Using Illegal Online Bus. Practices to Scam Consumers Nationwide (June 25, 2009), *available at* http://www.oag.state.ny.us/media_center/2009/june/june25b_09.html.

¹³⁴ *Id.*

¹³⁵ *Urban Nutrition, LLC*, No. 219 (ERSP Aug. 11, 2009), *available at* <http://www.narcpartners.org/ersp/list.aspx>.

¹³⁶ *Id.*

¹³⁷ 16 C.F.R. § 255.5 (2009).

¹³⁸ *Urban Nutrition, LLC*, No. 219 (ERSP Aug. 11, 2009), *available at* <http://www.narcpartners.org/ersp/list.aspx>.

¹³⁹ Will Greenwald, *All I Want for Christmas Is a PSP Viral-marketing Campaign*, CNET, Dec. 13, 2006, http://news.cnet.com/8301-17938_105-9667870-1.html.

advertising campaign.¹⁴⁰ After it was discovered that the campaign was the product of an advertising campaign, Sony faced widespread criticism on the Internet for creating the fake campaign.¹⁴¹

E. Liability for Investor Reliance on Employee Postings

Under regulations enforced by the Federal Securities and Exchange Commission (“SEC”), publicly traded companies must ensure that information that they disclose—particularly information that might be relied on by a potential investor in the company—is not fraudulent.¹⁴² The SEC has made clear that these antifraud provisions of federal securities law apply not only to traditional communications, but to online communications as well.¹⁴³ Of concern to companies was how to apply this requirement not only to blogs and electronic forums hosted by the company, but also to forums in which the company participates.¹⁴⁴ In recent guidance on this point, the SEC stressed that “companies are responsible for statements made by the companies, or on their behalf, on their Web sites or on third-party Web sites, and the antifraud provisions of the federal securities laws reach those statements.”¹⁴⁵

The SEC also gave specific guidance with respect to employees blogging on a third party’s website. Namely, the SEC further elaborated in its guidance that employees acting as representatives of a company cannot purport to speak in their “individual” capacities, and thus their statements are likely to be attributed to the company.¹⁴⁶ Such liability cannot be waived by asking a blog user not to make investment decisions based on the blog’s content or by disclaiming liability for any damages that may arise from use of the blog’s content.¹⁴⁷ For purposes of SEC requirements, then, an employee who engages in online blogging will likely be viewed as acting on behalf of the company, and as such, the company will want to ensure that those statements do not expose the employer to liability for securities fraud.

III. PRIVACY OBLIGATIONS

One of the greatest benefits to companies who create and use social networking and other online interactive marketing techniques is greater access to their customers and information about them. However, with this opportunity to collect significant information about customers comes some risks. For example, the CAN-SPAM Act¹⁴⁸ limits the manner in which companies can send electronic marketing

¹⁴⁰ *Id.*

¹⁴¹ *See, e.g., id.*

¹⁴² 17 C.F.R. § 240.10b-5 (2009).

¹⁴³ *See* Commission Guidance on the Use of Company Web Sites, 73 Fed. Reg. 45,862, 45,864 (Aug. 7, 2008) (to be codified at 17 C.F.R. pts. 241, 271).

¹⁴⁴ *Id.* at 45,870.

¹⁴⁵ *Id.* at 45,873.

¹⁴⁶ *Id.*

¹⁴⁷ *Id.*

¹⁴⁸ 15 U.S.C. §§ 7701–7713 (2006).

messages to their database of customers and potential customers.¹⁴⁹ In addition, there are a number of laws and initiatives aimed at protecting children's privacy that must be considered prior to engaging in interactive online marketing.¹⁵⁰

A. CAN-SPAM and Viral Marketing with Social Media

Laws have been enacted that impact how companies can interact with consumers, and those laws have implications in the social networking and blogging space. For example, the CAN-SPAM Act, which requires companies sending marketing emails to allow consumers to opt out of receiving future such emails,¹⁵¹ can impact a company that is planning an advertising campaign over social media.

The law has particular relevance for companies that encourage others to send marketing messages on its behalf. For example, if a company distributes free products to employees, and asks the employees to send emails to friends telling them their opinion of the product, the employer may be considered the "sender" of the email for CAN-SPAM purposes.¹⁵² Similarly, if a company asks users to send messages that contain the company's advertising, and gives the consumer something of value (like an extra entry into a sweepstakes), the company will be viewed as the "sender" of the message.¹⁵³ Consequently, the employer may have to scrub the email addresses selected by the employee or the consumer against the company's opt-out list, provide an electronic opt-out method in the message itself, provide the postal address of the company in the email, and make sure that the message is labeled an "advertisement."¹⁵⁴ This can be particularly difficult if the employee or consumer is sending the message directly from his or her own email program. These issues are compounded if the employee or consumer is sending the message through a social networking site using an "in" mail feature such as those found on LinkedIn or Facebook.

At least two cases have held that messages sent through social networking websites are subject to CAN-SPAM. For example, In *MySpace, Inc. v. Globe.com, Inc.*, MySpace, Inc. ("MySpace") filed an action against TheGlobe.com ("Globe") under CAN-SPAM (among other claims) alleging that Globe set up numerous dummy MySpace profiles and used the profiles to send almost 400,00 commercial e-messages marketing Globe products to MySpace users.¹⁵⁵ Globe argued that CAN-SPAM did not apply to its conduct because messages sent over MySpace's private messaging system are not e-mail subject to CAN-SPAM because: "(1) unlike email, MySpace e-messages have no real 'route' because the messages always remain within the 'walled garden' of MySpace; (2) MySpace e-messages are not email because they do not use simple mail transfer protocol ("SMTP"); and (3) unlike email addresses, MySpace e-message addresses have no domain part".¹⁵⁶ The court roundly rejected Globe's

¹⁴⁹ *Id.* § 7704(a).

¹⁵⁰ *Id.* §§ 6501–6506.

¹⁵¹ *Id.* § 7704(a)(3)(A).

¹⁵² *See id.* § 7702(16); 16 C.F.R. § 316.2(m) (2009).

¹⁵³ *See* 15 U.S.C. § 7702(16); 16 C.F.R. § 316.2(m).

¹⁵⁴ 15 U.S.C. § 7704(a).

¹⁵⁵ No. CV 06-3391-RGK (JCx), 2007 WL 1686966, at *1 (C.D. Cal. Feb. 27, 2007).

¹⁵⁶ *Id.* at *4.

arguments and concluded that the MySpace e-messages constituted electronic mail for purposes subject to CAN-SPAM.¹⁵⁷ Similarly, the court in *MySpace, Inc. v. Wallace* found that messages sent through MySpace’s internal messaging system constituted electronic mail subject to CAN-SPAM.¹⁵⁸

B. *Special Privacy Considerations for Children*

Companies that make products directed to children, or otherwise attractive to children, must consider a number of issues if they will be collecting personally identifiable information from or about children.¹⁵⁹ This is particularly true for social networking websites, *i.e.*, sites where users can freely interact with one another, whether they “know” the person or not. As many have concluded, when it comes to minors, interacting with strangers, whether online or offline, is not necessarily a good idea.¹⁶⁰

The largest and most well-known concern for such companies is the Children’s Online Privacy Protection Act (“COPPA”), which regulates the online collection and disclosure of personally identifiable information obtained from children under 13.¹⁶¹ In addition to COPPA, there have been a series of proposed state laws—one of which was recently enacted—that seeks to govern how and what information companies can collect from children.¹⁶² These laws were proposed in the wake of concerns over the limitations of COPPA, and its ability to protect children, particularly in the online social networking realm.¹⁶³ Finally, any company that engages in marketing activities towards children should be aware of the self-regulatory guidelines of the Children’s Advertising Review Unit, which include direction about how and what information should be collected from children under thirteen years old.¹⁶⁴

¹⁵⁷ *Id.* at *4–5.

¹⁵⁸ 498 F. Supp. 2d 1293, 1300–01 (C.D. Cal. 2007).

¹⁵⁹ See Children’s Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–6506 (2006).

¹⁶⁰ See, *e.g.*, Press Release, Senator John McCain, Senators McCain and Schumer Announce New Legislation Creating First-Ever Email Registry for Sex Offenders (Dec. 7, 2006) (on file with The John Marshall Law School), *available at* http://mccain.senate.gov/public/index.cfm?FuseAction=PressOffice.PressReleases&ContentRecord_id=60B748CD-BC58-4833-8D5D-15C9C3132D40 (discussing legislation that requires registered sex offenders to register their email addresses).

¹⁶¹ 15 U.S.C. §§ 6501–6506.

¹⁶² See, *e.g.*, ME. REV. STAT. ANN. tit. 10, §§ 9551–54 (2009).

¹⁶³ Compare, *e.g.*, *id.* § 9552(1) (“It is unlawful for a person to knowingly collect or receive health-related information or personal information for marketing purposes from a minor without first obtaining verifiable parental consent of that minor’s parent or legal guardian.”), with 15 U.S.C. § 6502(a)(1) (“It is unlawful for an operator of a website or online service directed to children, or any operator that has actual knowledge that it is collecting personal information from a child . . .”). See also Justin Ellis, *New Maine Law Spins a Tangled Web*, PORTLAND PRESS HERALD (ME.), Aug. 24, 2009, at A1 (reporting that the intent of Maine’s law is to “expand on COPPA”).

¹⁶⁴ See generally CHILDREN’S ADVER. REVIEW UNIT, SELF-REGULATORY PROGRAM FOR CHILDREN’S ADVER. (2009) [hereinafter *CARU Guidelines*], *available at* <http://www.caru.org/guidelines/guidelines.pdf> (offering guidance to assist advertisers and “promote responsible children’s advertising”).

1. COPPA—The Starting Line

Under COPPA (and the FTC’s Final Rule implementing that Act),¹⁶⁵ companies that operate websites that are directed to—or appealing to—children which collect personal information from children online must first obtain verifiable parental consent to collect such information.¹⁶⁶ There are some limited exceptions to this requirement, including cases where the information is being collected in order to obtain consent.¹⁶⁷

There are two types of parental consent that a company can obtain—level one and level two (commonly referred to as the “sliding scale approach”).¹⁶⁸ Level one is consent provided by email, such as the parent sending an email stating that he or she grants consent, plus a “more secure” mechanism such as sending a follow-up email 24 hours later confirming that the parent granted consent.¹⁶⁹ Level two, a more secure mechanism of granting consent, is necessary if the child’s information will be disclosed to third parties—or if the child will be able to disclose his or her information to third parties.¹⁷⁰ Such disclosure is typical in a social networking site, for example, where a child can send free text messages to other users (and in those free text messages could disclose personally identifiable information). To obtain level two consent, a company can either have a parent send in a physically signed consent form by mail or fax, have a parent call and provide verbal consent, or give consent “through a credit card transaction.”¹⁷¹ The FTC’s COPPA Rule anticipates that other mechanisms of “more secure consent” may be developed, although most companies opt for signed consent forms or verbal consent.¹⁷²

To adhere to COPPA, companies that collect personally identifiable information from children under age thirteen must also follow six basic requirements: (1) notify parents prior to collecting information from their children; (2) obtain parental consent prior to collecting personal information from children (as described above); (3) maintain control of the child’s information; (4) not condition the child’s participation on the submission of excessive information; (5) maintain the security of personal information submitted by the child; and (6) post a privacy policy on the homepage of the website and link to the privacy policy on every page on which personal information is collected.¹⁷³

Since COPPA was passed, the FTC has brought actions against companies for a variety of violations of the act, primarily stemming from the companies’ failure to obtain verifiable prior parental consent. For example, one company simply told children on its website to “ask your parents’ permission” before signing up; the FTC argued that this did not constitute verifiable parental consent, and the parties settled

¹⁶⁵ 15 U.S.C. §§ 6501–6506; Children’s Online Privacy Protection Rule, 16 C.F.R. pt. 312 (2009).

¹⁶⁶ 16 C.F.R. § 312.5(a)(1).

¹⁶⁷ *Id.* § 312.5(c).

¹⁶⁸ *See id.* § 312.5(b)(2).

¹⁶⁹ *See id.*

¹⁷⁰ *See id.*

¹⁷¹ *Id.*

¹⁷² *See id.*

¹⁷³ 15 U.S.C. § 6502(b)(1) (2006); 16 C.F.R. § 312.3.

with a payment by the company of \$35,000 in civil penalties.¹⁷⁴ In a similar case, another company instructed children under thirteen years old to have their parents fill in an online parental consent form, but took no steps to ensure that a parent actually saw or filled out the forms.¹⁷⁵ That case was settled with a payment of \$85,000 in civil penalties.¹⁷⁶

One option for companies is to avoid collecting personal information from children under thirteen years old by creating an “age block,” i.e., asking a user how old he or she is, and if the answer is “under 13,” not permitting the user to provide personally identifiable information. Companies that ask age, however, will be deemed to be on notice that a user is under thirteen years old if the user so indicates, and will need to take steps after the information has been provided to block the user from providing personal information. This can be done by dropping a session cookie stopping the person from submitting information during the same browser session. It is this second option that many social networking sites, and other sites intended for older audiences but appealing to younger ones, have taken.

For example, in 2006, the FTC announced a settlement with Xanga.com, a social networking site that it felt was appealing to children under age thirteen, even though it was directed to adults.¹⁷⁷ According to the FTC, Xanga.com had actual knowledge that children under thirteen years old were registering for the social networking site, because it asked individuals to provide their birth date during the registration process, but nevertheless failed to block children under age thirteen or obtain prior verifiable parental consent as required by COPPA.¹⁷⁸ As part of the settlement, Xanga.com agreed to pay a \$1 million civil penalty.¹⁷⁹

2. Growing Concern over COPPA’s Limitations—States Take Action

As social networking became more popular, many began to feel that COPPA’s protections were not enough.¹⁸⁰ Children could too easily lie about their age, gain access to these sites, and find themselves in danger.¹⁸¹ In the wake of those fears,

¹⁷⁴ See Complaint at 3 ¶ 14, *United States v. Ohio Art Co.*, No. 3:02-CV-7203 (N.D. Ohio 2002 Apr. 22, 2002); Consent Decree, *United States v. Ohio Art Co.*, Case No. 3:02-CV-7203 (N.D. Ohio 2002 Apr. 22, 2002).

¹⁷⁵ See Complaint at app. Ex. C, *United States v. Hershey Foods Corp.*, No. 4:CV03-350 (M.D. Pa. Feb. 26, 2003), available at <http://www.ftc.gov/os/caselist/hershey/030227herseyexhibit.pdf>.

¹⁷⁶ See Consent Decree, *United States v. Hershey Foods Corp.*, No. 4:CV03-350 (M.D. Pa. Feb. 26, 2003).

¹⁷⁷ Press Release, Fed. Trade Comm’n, Xanga.com to Pay \$1 Million for Violating Children’s Online Privacy Protection Rule (Sept. 7, 2006) (on file with the John Marshall Review of Intellectual Property Law), available at <http://www.ftc.gov/opa/2006/09/xanga.shtm>.

¹⁷⁸ Complaint at 5–8, *United States v. Xanga.com, Inc.*, No. 06-6853 (SHS) (S.D.N.Y. Sept. 7, 2006).

¹⁷⁹ Consent Decree & Order for Civil Penalties, Injunction, & Other Relief at 5, *United States v. Xanga.com, Inc.*, No. 06-6853 (SHS) (S.D.N.Y. Sept. 7, 2006), available at <http://www.ftc.gov/os/caselist/0623073/xangaconsentdecree.pdf>; see Press Release, Fed. Trade Comm’n, *supra* note 177.

¹⁸⁰ See, e.g., Justin Ellis, *supra* note 163.

¹⁸¹ See, e.g., John B. Kennedy & Mary Wong, *Recent Developments in U.S. Privacy Law, Including Post-September 11, 2001*, in THIRD ANNUAL INSTITUTE ON PRIVACY LAW: NEW DEVELOPMENTS & ISSUES IN A SECURITY-CONSCIOUS WORLD, at 11, 50 (PLI Patents, Copyrights,

forty-nine state attorneys general—with Texas as the lone state holdout—pursued MySpace, a popular social networking site.¹⁸² In January 2008, the parties reached an agreement regarding how the site—and its competitors—would handle online child safety.¹⁸³ As part of the agreement, the parties issued a Joint Statement on Key Principles of Social Networking Site Safety, in which MySpace agreed to organize an industry-wide task force to study the issue of child safety on social networking sites.¹⁸⁴

The key principles included using tools to protect children from inappropriate content and inappropriate adult contacts, and the education of parents, children, and teachers about online safety.¹⁸⁵ As part of the settlement with the Attorneys General, MySpace also made modifications to its site to block users over eighteen years old from browsing those under eighteen, prohibiting users over eighteen from adding friends under sixteen unless the user knows the friend's last name or e-mail address, and prohibiting users under eighteen from accessing tobacco advertisements and those under twenty-one from accessing alcohol advertisements.¹⁸⁶ The Texas attorney general stated that he did not sign the agreement for fear that it would give parents and children a false sense that children would be secure.¹⁸⁷

After the settlement, an Internet Safety Technical Task Force was assembled to consider the practical limitations and difficulties that age verification presents.¹⁸⁸ A December 31, 2008, report produced by the Task Force did not provide many alternate suggestions, concluding only that “[a]ge verification and identity authentication technologies are appealing in concept but challenged in terms of effectiveness.”¹⁸⁹ The Task Force also noted that the best solution for protecting children online consists of a combination of technical solutions, education, parental oversight, law enforcement, and “sound” policies from social networking websites.¹⁹⁰

In a nod, perhaps, to the missing details of the Task Force, a number of states have proposed laws that go beyond COPPA, hoping to better protect children under

Trademarks, & Literary Property Course, Handbook Series No. G0-00W2, 2002), *available at* WL 701 PLI/Pat 11.

¹⁸² MYSPACE & ATTORNEYS GEN., JOINT STATEMENT ON KEY PRINCIPALS OF SOC. NETWORKING SITES SAFETY 4–6 (2008), *available at* <http://www.ag.state.mn.us/PDF/PressReleases/SocialNetworkingSitesSafety.pdf> [hereinafter JOINT STATEMENT]; *see* Anne Barnard, *MySpace Agrees to Lead Fight to Stop Sex Predators*, N.Y. TIMES, Jan. 15, 2008, at B3; Brad Stone, *Facebook Agrees to Devise Tools to Protect Young Users*, N.Y. TIMES, May 9, 2008, at C4.

¹⁸³ JOINT STATEMENT, *supra* note 182, at 1–2; Barnard, *supra* note 182.

¹⁸⁴ JOINT STATEMENT, *supra* note 182, at 1; Barnard, *supra* note 182; *see also* Brad Stone, *Despite News Reports, Task Force Finds Online Threat to Children Overblown*, N.Y. TIMES, Jan. 14, 2009, at A16 (“A task force created by 49 state attorneys general to look into the problem of sexual solicitation of children online has concluded that there really is not a significant problem.”).

¹⁸⁵ JOINT STATEMENT, *supra* note 182, at 1–3.

¹⁸⁶ *Id.* app. A.

¹⁸⁷ Press Release, Tex. Att’y Gen., Att’y Gen.’s Fugitive Unit Arrests Sex Offender Using MySpace; Abbott Objects to Recent Report (Feb. 4, 2009) (on file with The John Marshall Review of Intellectual Property Law).

¹⁸⁸ *See generally* INTERNET SAFETY TECHNICAL TASK FORCE, ENHANCING CHILD SAFETY & ONLINE TECHNOLOGIES (2008), *available at* <http://cyber.law.harvard.edu/pubrelease/isttf> (presenting the findings of the task force).

¹⁸⁹ *Id.* at app. D (stating this as the Technology Advisory Board’s conclusion to its part of the task force’s study).

¹⁹⁰ *Id.* at 6.

thirteen years old in their states who provide personally identifiable information online to sites—including social networking sites. These states include: Illinois (would require social networking sites to get written parental permission before a minor can create a profile page, and would require parents to be provided with ongoing access to their children’s pages);¹⁹¹ Georgia (would prohibit social networking sites from allowing minors to create profiles without first obtaining parental consent, and without giving parents ongoing access to the minor’s profile);¹⁹² and New Jersey (would require websites that collect information from children between 13 and 17 to obtain verifiable parental consent for the collection, use, and disclosure of adolescents’ information).¹⁹³ and North Carolina (would have required all social networking sites to obtain parental consent before a minor could use their sites, and would have required procedures to confirm age and identities of parents).¹⁹⁴ As of this writing, only the Illinois bill, as originally proposed and described here, remains pending.

In an interesting twist, a more restrictive version of these states’ laws was passed this summer in Maine, and as of this writing (despite emergency motions filed against it)¹⁹⁵ took effect on September 12, 2009.¹⁹⁶ The Maine law brings four new features to the table. First, it goes beyond the online world and puts restrictions on offline interaction with minors.¹⁹⁷ Second, it expands the age of applicability to eighteen years of age, up from COPPA’s thirteen.¹⁹⁸ Third, it puts an absolute prohibition on direct marketing to children under eighteen years old—whether parental permission has been obtained or not.¹⁹⁹ The type of prohibited direct marketing is broadly defined, and would presumably include not just email and text messages sent to children in Maine—including those between thirteen and seventeen, but also marketing messages sent directly to a child through social networking websites like Facebook and Twitter.²⁰⁰ This brings into question how companies will handle existing databases that may contain information of children less than eighteen years old who reside in Maine. Fourth, the law prohibits collecting personal information from children in Maine under eighteen for “marketing purposes” without first obtaining parental consent.²⁰¹ The definition of “marketing purposes” is quite broad, and is not to be confused with direct marketing

¹⁹¹ Social Networking Website Access Restriction Act, H.B. 1312, 96th Gen. Assem., Reg. Sess. (Ill. 2009).

¹⁹² A Bill to Be Entitled, S.B. 59, 149th Gen. Assem., Reg. Sess. (Ga. 2007).

¹⁹³ Adolescents’ Online Privacy Protection Act, A108, 108th Gen. Assem. (N.J. 2008).

¹⁹⁴ Protect Children from Sexual Predators Act, S.B. 2007-132, Reg. Sess. (N.C. 2007) (enacted), available at <http://www.ncga.state.nc.us/Sessions/2007/Bills/Senate/PDF/S132v6.pdf>. As enacted, the law only requires social network website operators to take reasonable efforts to prevent registered sex offenders from accessing their sites. *Id.*

¹⁹⁵ See Plaintiffs’ Motion for Preliminary Injunction, Me. Indep. Colls. Ass’n v. Baldacci, No. CV-09-396-B-W (D. Me. Aug. 26, 2009); Memorandum in Support of Plaintiffs’ Motion for Preliminary Injunction, Me. Indep. Colls. Ass’n v. Baldacci, No. CV-09-396-B-W (D. Me. Aug. 26, 2009).

¹⁹⁶ ME. REV. STAT. ANN. tit. 10, §§ 9551–54 (2009).

¹⁹⁷ *Id.* §§ 9552–53.

¹⁹⁸ See *id.* (protecting “minors” from unlawful collection and use of health-related information or personal information, and prohibiting predatory marketing against “minors”).

¹⁹⁹ *Id.* § 9553.

²⁰⁰ See *id.*

²⁰¹ See *id.* § 9552(1).

to the child from whom information was collected (which, as mentioned above, is prohibited under this law, whether or not consent has been obtained).²⁰² Instead, marketing covers generally the “purposes of marketing or advertising products, goods or services to individuals.”²⁰³ Thus, if a minor’s personal information is collected, analyzed, and used internally to determine how to market to individuals generally, parental consent would arguably be necessary under the new law.

The Maine Attorney General is given authority to enforce the law, with potential civil penalties of \$10,000 to \$20,000 for the first violation, and \$20,000 or more for the second or subsequent violation of the law.²⁰⁴ The office of the Maine Attorney General has indicated that it will not enforce the law.²⁰⁵ However, the new law provides for a private right of action, with statutory damages of up to \$250 for each violation.²⁰⁶ In an effort to discourage such private suits, the District Court of Maine, in responding to an emergency suit filed against the law, recently found that the plaintiffs met their burden of establishing a likelihood of success on the merits of their claims that the law is overbroad and violates the First Amendment.²⁰⁷ The court ultimately dismissed the lawsuit upon stipulation of the parties, and warned anyone considering bringing a private action that it would give the same analysis (that the law is likely unconstitutional) if they decided to bring a case.²⁰⁸ Presumably, with this ruling in place, the Maine legislature may look to repeal or revise the law.²⁰⁹

3. *The Children’s Advertising Review Unit*

As laws regarding information collection from minors are constantly in flux, it is always helpful for companies to have an overarching guide they can turn to in the hopes of avoiding not just a violation of a current law, but a violation of a law that might not yet be in place. Given that such laws may apply retroactively to information already collected—such as the Maine law described above—these guides take on newfound importance.²¹⁰ One such guide was developed by the Children’s Advertising Review Unit (“CARU”), a self-regulatory body funded by companies that advertise to children, or whose products are appealing to children.²¹¹ As part of its self-regulatory mission, CARU publishes the CARU Self-Regulatory Guidelines

²⁰² *Id.* §§ 9551(2), 9553.

²⁰³ *Id.* § 9551(2).

²⁰⁴ *Id.* § 9554.

²⁰⁵ Stipulated Order of Dismissal at 1, *Me. Indep. Colls. Ass’n v. Baldacci*, No. CV-09-396-B-W (D. Me. Sept. 9, 2009).

²⁰⁶ ME. REV. STAT. ANN. tit. 10, § 9553 (2009).

²⁰⁷ Stipulated Order of Dismissal, *supra* note 205, at 1.

²⁰⁸ *Id.*

²⁰⁹ See Christopher Cousins, *Law Protecting Minors’ Health Data Not to Be Enforced*, BANGOR DAILY NEWS (ME.), <http://www.bangordailynews.com/detail/119741.html> (last visited Nov. 9, 2009) (“Schneider [author of the bill] ... hope[s] that more representatives from the affected industries will participate in the process of revamping the law.”).

²¹⁰ *But see* *Bowen v. Georgetown Univ. Hosp.*, 488 U.S. 204, 208 (1988) (“Retroactivity is not favored in the law. Thus, congressional enactments and administrative rules will not be construed to have retroactive effect unless their language requires this result.”).

²¹¹ CARU GUIDELINES, *supra* note 164.

(“Guidelines”), which it has updated frequently over the years to address new developments in child marketing, including online information collection.²¹²

The Guidelines touch on all aspects of marketing and advertising to children, including interactive and online marketing campaigns, and contain guidelines on Interactive Electronic Media.²¹³ Under the Guidelines, companies that collect information from children must follow, essentially, the requirements of COPPA.²¹⁴ The Guidelines provide more information about how a company can take actions such as screening for users under thirteen years old and blocking them from accessing a company’s website.²¹⁵ In addition to providing more direction about following COPPA, CARU is also active in policing the industry for violations. For example, in a 2007 decision, CARU announced that it was referring WUK Music Group’s daechelle.com, a fan site for the singer Daechelle, to the FTC after finding that the site collected personal information and asked children for their ages without obtaining verifiable parental consent.²¹⁶ Although the advertiser included the statement, “You must be 13 years of age or older to submit personal information,” people who were identified as being under thirteen were not blocked from joining the site.²¹⁷ Because the operator of the site failed to comply with CARU’s recommendation that the site implement neutral age screening and block users under thirteen years of age from registering, CARU recommended the case to the FTC.²¹⁸

Companies often work with CARU, however, obviating the need for the entity to refer a company to the FTC for further action. For example, in August 2009, CARU recommended to the Sandylion Sticker Designs website that it modify its information collection practices, and the company agreed to do so.²¹⁹ In that case, if a child indicated that he or she was under the age of thirteen, the child could circumvent the need to fill out the parent registration form on the site by clicking the back button and entering a date of birth that made him or her over thirteen.²²⁰ CARU indicated that it was concerned about the inclusion of “tip-off” language that encouraged children to misstate their ages and the lack of a session cookie to block the attempts at circumvention of the age verification process.²²¹

²¹² See generally *id.* (instructing companies who market towards children what the standard for advertising to children is and how to comply with current laws).

²¹³ *Id.* at 11–15.

²¹⁴ Compare *id.* (discussing inappropriate advertising to children and providing guidance regarding online privacy protection for children under the age of thirteen), with 15 U.S.C. § 6502 (2006) (protecting children under the age of thirteen from unfair and deceptive acts and practices on the internet in connection with the collection and use of personal information), and 16 C.F.R. § 312.5 (2009) (listing the general requirements for parental consent).

²¹⁵ CARU GUIDELINES, *supra* note 164, at 15.

²¹⁶ Press Release, CARU News, CARU Refers Daechelle Fan Site to FTC for Review (Nov. 6, 2007) (On file with The John Marshall Review of Intellectual Property Law), available at <http://www.caru.org/news/2007/CARU-4739PR.pdf>.

²¹⁷ *Id.*

²¹⁸ *Id.*

²¹⁹ Press Release, CARU News, CARU Recommends Sandylion Modify Website to Better Protect Children’s Privacy; Company Agrees to Do So (Aug. 18, 2009) (on file with The John Marshall Review of Intellectual Property Law), available at <http://www.caru.org/news/2009/5048PR.pdf>.

²²⁰ *Id.*

²²¹ *Id.*

CARU has also recommended modifications to websites that contain links to third-party sites that are not compliant with CARU's guidelines. For example, in August 2009, CARU reviewed a website owned by Kidz Bop LLC, and discovered that the site included a link to a third-party mobile website operated by Gameloft.²²² CARU determined that Gameloft's site was not in compliance with CARU's guidelines with respect to online privacy protection.²²³ The non-compliant website did not implement a neutral age-screening mechanism to filter children under thirteen years old, and various areas of the site collected personally identifiable information.²²⁴ CARU found that Kidz Bop could reasonably expect children under thirteen to visit their website and CARU guidelines specifically provide that operators of websites which are for children or contain areas for children should not knowingly link to other websites that do not comply with CARU guidelines.²²⁵

Methods for collecting verifiable parental consent—and screening children who are under thirteen (or eighteen, or any other age)—are not foolproof.²²⁶ Nevertheless, companies that collect information online from children will be found responsible if they do not screen and/or obtain parental consent successfully, with states seeking more and more to turn that responsibility into something resembling absolute liability.²²⁷ This is particularly true for entities that set up forums for third parties to interact—like social networking sites.²²⁸ As a result, companies should look not only to existing laws and pending legislation for direction when creating online information, but also stay current with self-regulatory guidance and cases.

CONCLUSION

Corporate blogs, social networking sites, and a wide array of other new media communication tools allow companies to advertise to and directly interact with their customers. As companies engage with consumers in these new media, however, they need to keep in mind the legal risks that are involved, and should take steps to limit their liability when possible. And, such limitations and steps do exist, even if this area of the law is still developing.

²²² Press Release, CARU News, CARU Recommends Kidz Bop Modify Website to Better Protect Children's Privacy; Company Agree to Do So (June 24, 2009) (on file with The John Marshall Review of Intellectual Property Law), *available at* <http://www.caru.org/news/2009/5034PR.pdf>.

²²³ *Id.*

²²⁴ *See id.*

²²⁵ CARU GUIDELINES, *supra* note 164, at 15.

²²⁶ *See* 15 U.S.C. § 6501 (9) (2006) (defining "verifiable parental consent" using the term "reasonable").

²²⁷ *Id.* § 6502(a)–(c).

²²⁸ *See* HOW TO COMPLY, *supra* note 4, at 1 (defining "Who Must Comply" with COPPA and COPPR).