Monday, October 1, 2012
2:30 PM - 4:00 PM

902 – The Advertising Report

Tristan Ostrowski
Product Counsel - Android
Google, Inc.

Todd Vare
Partner
Barnes & Thornburg LLP

Faculty Biographies

Tristan Ostrowski

Tristan Ostrowski is a product counsel for Android on the Google legal team in Mountain View, CA. He works with the Android product, engineering, and policy teams on legal issues related to feature development, product launches, geographic expansion, and marketing. He also advises on issues faced by Android app developers, device manufacturers, and carriers. In this role, he has focused on IP, privacy, content regulation and consumer protection issues relating to Google Play and the Android platform. Prior to joining Google, he worked as an IP attorney at Cleary Gottlieb Steen & Hamilton in New York.

Mr. Ostrowski has a BA and a BS from Arizona State University, and is a graduate of New York University School of Law.

Todd Vare

Todd G. Vare is a partner resident in the Indianapolis office of Barnes & Thornburg LLP. Mr. Vare represents clients in the protection and enforcement of intellectual property rights in trial and appellate courts around the country, and was listed in the 2012 edition of *Best Lawyers in America*.

Mr. Vare has litigated patent disputes covering a wide variety of technologies, including herbicides/pesticides, dielectric fluids, genetics, pharmaceuticals, medical devices, telecommunications, microprocessor and integrated circuit designs, software programs and processes, cellular antenna systems, and mechanical devices. Mr. Vare also represents clients in disputes involving trademarks, copyrights, trade secrets, software performance, software licenses, employee non-compete and non-disclosure agreements, and rights of publicity.

In addition to trial work, Mr. Vare argued before the United States Supreme Court in U.S. v. Santos, (opinion issued June 2, 2008) which resulted in a victory for his client involving the scope of the federal money laundering statute. Mr. Vare also has represented clients in appeals in the 7th Circuit, the Federal Circuit, the 11th Circuit, and the Indiana Court of Appeals.

Mr. Vare serves as co-chair of the nanotechnology group and business and technology group of Barnes & Thornburg, and additionally is active in the firm's life sciences group.

Mr. Vare received his JD, summa cum laude, from Indiana University School of Law - Indianapolis. He graduated from Miami University with a BA in international studies. He also received an MBA from the Indiana University school of business, and worked in advertising and marketing communications before attending law school.

Legal Implications Affecting Mobile Applications and Social Media in Advertising

Todd G. Vare
Partner, Intellectual Property
Barnes & Thornburg LLP

I. Introduction

As the Internet becomes increasingly mobile and social, businesses have adapted to take advantage of new ways to communicate with and influence their customers. Now, advertisers have the ability to bid on advertising space in real time, based on detailed information about specific individuals.[1] Consumers carry the Internet with them in their pockets, which not only gives them the ability to communicate and to consume information more readily than at any other time in history, but also provides businesses with the ability to reach particular consumers wherever they may be. As technology has evolved, a complex and rapidly changing body of laws has developed to regulate it. Some, such as the Federal Trade Commission Act, are old laws adapted to new circumstances. Others, such as the Children's Online Privacy Protection Act and Gramm-Leach-Bliley Act, are new laws designed to address emerging issues. A number of regulatory agencies, such as the Federal Trade Commission, United States Copyright Office, and National Labor Relations Board, have become responsible for supervising companies and adapting a complex body of administrative rules to suit novel challenges. The following materials are intended to highlight a few[2] important and emerging legal issues that may put companies at risk as they negotiate the new media landscape.

---

[1] Julia Angwin, *Online Tracking Ramps Up: Popularity of User-Tailored Advertising Fuels Data Gathering on Browsing Habits*, THE WALL STREET JOURNAL, June 17, 2012, http://www.wsj.com/article/SB10001424052702303836404577472491637833420.html.

[2] These materials are not meant to be exhaustive, but rather to provide a brief but focused analysis of a few of the most salient current issues.

II. Advertising: Privacy and Endorsements

A. The Changing Landscape

Consumers are increasingly interconnected through social media and internet-capable mobile devices. To better and more effectively ply their goods and services, businesses have gained access to a vast array of data regarding current and potential customers. According to one recent study, the average visit to a web page triggered fifty-six instances of data collection related to online advertising or marketing.[3] There is obvious value in being able to target consumers based on such granular knowledge of their habits and preferences, and it is not surprising, therefore, that online advertising has grown to become a $31 billion business.[4] Outside of the advertising context, businesses of all sorts may collect consumer financial information, personal health information, or other forms of data that allow them to build relationships with their customers and go about their business. Much of this information can be monetized, and there are strong incentives for companies to collect valuable consumer personal data either to use in-house or to sell to third-parties. Companies are not the only parties interested in this deluge of personal data, however, and online collection of consumer data has given rise to increased scrutiny from the Federal Trade Commission, consumer sensitivity to online privacy, and a series of policy initiatives from the states and federal government that create a variety of potential pitfalls for companies seeking to exploit the rapidly evolving media landscape.

This has been particularly true in the mobile space, where it is estimated that 98 billion mobile apps will be downloaded by 2015.[5] Given the scope of the mobile app marketplace,

[3] Julia Angwin, *supra* note 1.

[4] *Id.*

[5] Press Release, Office of the Attorney General, State of California, Attorney General Kamala D. Harris Secures Global Agreement to Strengthen Privacy Protections for Users of Mobile Applications (Feb. 22, 2012) (on file with author), *available at* http://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-secures-global-agreement-strengthen-privacy.

increased consumer sensitivity to businesses' privacy practices has driven sweeping policy initiatives. The California Online Privacy Protection Act, for example, requires any operator of a commercial website or an online service that collects personally identifiable information to "conspicuously post its privacy policy."[6] The Attorney General of California interprets this Act to extend to mobile applications that collect personal data from California consumers, and recently established a new Privacy Enforcement and Protection Unit which will "focus on protecting consumer and individual privacy through civil prosecution of state and federal privacy laws."[7] California has also pushed market leaders in the mobile app industry to adopt improved privacy protections.[8] In February, the Attorney General of California and industry leaders Amazon, Apple, Google, Hewlett-Packard, Microsoft, and Research in Motion signed a Joint Statement of Principles committing themselves to develop best practice for mobile privacy and promote greater privacy transparency among their app developers.[9] A series of recent policy statements demonstrates that the federal government is also moving toward requiring businesses to be more transparent and to provide their customers greater control over mobile apps' use of their personal information.[10]

When companies collect information from individuals who visit their websites or use their services, they are constrained in their use and maintenance of that data by the Federal Trade

---

[6] CAL. BUS. & PROF. CODE § 22575(a) (West 2012).

[7] *Attorney General Kamala D. Harris Announces Privacy Enforcement and Protection Unit*, INLAND VALLEY NEWS (July 25, 2012), http://www.inlandvalleynews.com/2012/07/25/attorney-general-kamala-d-harris-announces-privacy-enforcement-and-protection-unit.

[8] Press Release, *supra* note 5.

[9] Joint Statement of Principles, Office of the Attorney General, State of California (Feb. 22, 2012) (on file with author), *available at* http://oag.ca.gov/system/files/attachments/press_releases/n2630_signed_agreement.pdf.

[10] *See, e.g.*, FEDERAL TRADE COMMISSION, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS (2012); THE WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY (2012).

Commission Act, state laws, and a series of industry-specific rules and statutes. For example, Apple, Inc. is currently defending a class action in which the plaintiffs allege that it violated mobile device users' privacy rights under federal and state law by allowing third-party applications to collect and use personal information without user consent or knowledge.[11] A California federal judge recently denied Apple's motion to dismiss, ruling that claims against Apple for violations of the California Unfair Competition Law (creating causes of action for business practices that are unlawful, unfair, or fraudulent)[12] and Consumer Legal Remedies Act (prohibiting unfair methods of competition and unfair or deceptive acts or practices)[13] could proceed.[14] The Federal Trade Commission has consistently brought actions for privacy violations, notably against Facebook, Myspace, and Twitter.[15] These actions may result in civil penalties[16] and often create ongoing obligations for targeted companies (e.g., having to submit to regular privacy audits for several years).[17]

These potential liabilities are based on an array of state and federal privacy law that governs companies' collection and use of data. Much of this law regulates specific industries, service providers, or types of information.[18] However, the Federal Trade Commission Act

[11] *See In re* iPhone Application Litig., No. 11-MD-02250-LHK, 2012 WL 2126351 (N.D. Cal. June 12, 2012) (granting partial summary judgment in favor of defendants, but holding that plaintiffs' claims under California's Consumer Legal Remedies Act and Unfair Competition law could proceed).

[12] Cal. Bus. & Profs. Code § 17200

[13] Cal. Civ. Code § 1750

[14] *In re* iPhone Application Litig., 2012 WL 2126351, at *1.

[15] Complaint, *In re* Myspace LLC, No. 102-3058, 2012 WL 1745313 (F.T.C May 8, 2012); Complaint, *In re* Facebook, Inc., No. 092-3184, 2011 WL 7096348 (F.T.C. Nov. 29, 2011); Complaint, *In re* Twitter, Inc., No. C-4316, 2011 WL 914034 (F.T.C. June 24, 2010).

[16] *See, e.g.*, United States v. Playdom, Inc., No. SACV-11-0724-AG (ANx) (C.D. Cal. May 24, 2011) (consent decree) (ordering the defendant, a website operator, to pay a civil penalty of $3,000,000 for violations of the Children's Online Privacy Protection Act).

[17] *See, e.g.*, *In re* Twitter, Inc., No. C-4316, 2011 WL 914034 (F.T.C. Mar. 2, 2011) (consent decree).

[18] *See, e.g.*, Fair Credit Reporting Act (FCRA), 15 U.S.C. §§ 1681-1681y (2006) (imposing requirements on all persons who furnish information to consumer reporting agencies); Family Educational Rights and Privacy Act

(FTCA), which prohibits unfair or deceptive practices, gives the Federal Trade Commission broad authority to require organizations to maintain reasonable privacy policies and to ensure compliance with organizations' representations to users regarding the collection and use of personally identifiable information, because failure to do so is considered deceptive.[19] Because of its broad prohibition on unfair and deceptive practices, the FTCA therefore gives rise to broad legal implications for companies that collect or store consumer information.

B. General Privacy Risks

In general, a company may incur legal liability under the Federal Trade Commission Act when it (1) fails to honor the representations it makes to consumers regarding the collection and use of their personal data, or (2) fails to take reasonable precautions to safeguard sensitive consumer data.

The privacy laws that may apply in such situations are primarily concerned with user data that can be linked to an individual. This information is usually called "personally identifiable information" or "personal identification information" (PII). PII has been defined in a variety of ways. The Children's Online Privacy Protection Act, for example, defines PII as

> individually identifiable information about an individual collected online, including a first and last name; a home or other physical address including street name and name of a city or town; an e-mail address; a telephone number; a Social Security number; any other identifier that the Commission determines permits the physical or online contacting of a specific individual; or information concerning the child or the parents of that child that the website collects online from the child and combines with an identifier described in this paragraph.[20]

The National Institute of Standards and Technology uses a broader definition:

(FERPA), 20 U.S.C. § 1232g (2006) (imposing, among other requirements, restrictions on schools' release of students' personal information).

[19] 15 U.S.C. § 45(a) (2006).

[20] 15 U.S.C.A. § 6501(8) (West 2012) (internal subdivisions omitted).

> [Personally Identifiable Information] is any information about an individual . . . , including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mothers' maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.[21]

State laws also include broad definitions of PII. The Supreme Court of California, for example, recently held that an individual's zip code is PII.[22] Finally, the Federal Trade Commission's recent policy recommendations indicate that the Commission's focus is on the "collect[ion] or use [of] consumer data that can be *reasonably linked* to a specific consumer, computer, or other device."[23] The various definitions are consistent in that they focus on information that either identifies a specific person or can be combined with other information to determine that specific person's identity.

When a company makes claims regarding its collection and use of user data, it is required to honor its promises. Any company that does not honor its own privacy policies exposes itself to an enforcement action by the Federal Trade Commission, which has primary responsibility for

---

[21] ERIKA MCCALLISTER, TIM GRANCE & KAREN SCARFONE, COMPUTER SECURITY DIVISION, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, GUIDE TO PROTECTING THE CONFIDENTIALITY OF PERSONALLY IDENTIFIABLE INFORMATION (PII): RECOMMENDATIONS OF THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY ES-1 (2010).

[22] *See* Pineda v. Williams-Sonoma Stores, 51 Cal. 4th 524, 527-28 (2011).

[23] FEDERAL TRADE COMMISSION, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS 21 (2012) (emphasis added).

policing compliance with federal Internet privacy law.[24] This authority is derived from the FTCA's prohibition on unfair or deceptive practices.[25].

The Federal Trade Commission will find deception where "there is a representation, omission, or practice that is likely to mislead the consumer acting reasonably in the circumstances, to the consumer's detriment."[26] Failure to adhere to a privacy policy is considered a deceptive practice and may give rise to a privacy suit initiated by the Federal Trade Commission.[27] Moreover, the Federal Trade Commission considers a practice unfair if it "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and is not outweighed by countervailing benefits to consumers or competition."[28] A company may run afoul of the FTC when it fails to take adequate precautions to protect consumer data.[29] The Federal Trade Commission has brought a number of these actions in recent years.[30]

---

[24] *See* Federal Trade Commission, *Making Sure Companies Keep Their Privacy Promises to Consumers*, FTC.GOV, http://www.ftc.gov/opa/reporter/privacy/privacypromises.shtml (last visited June 28, 2012) ("When companies tell consumers they will safeguard their personal information, the FTC can and does take law enforcement action to make sure that companies live up to these promises. As of May 1, 2011, the FTC has brought 32 legal actions against organizations that have violated consumers' privacy rights, or misled them by failing to maintain security for sensitive consumer information.").

[25] 15 U.S.C. § 45(a) (2006) ("Unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful. The [Federal Trade Commission] is hereby empowered and directed to prevent [such acts or practices].")

[26] Federal Trade Commission, FTC Policy Statement on Deception, Letter from Fed. Trade Comm'n to Hon. John D. Dingell, Chairman, H. Comm. On Energy and Commerce (Oct. 14, 1983), *available at* http://www.ftc.gov/bcp/policystmt/ad-decept.htm.

[27] *See, e.g.*, Complaint at 5-6, *In re* Upromise, Inc., No. C-4351, 2012 WL 91365, at *4 (F.T.C. Jan. 5, 2012) (stating that the defendant's failure to adhere to its representations regarding privacy and data security was "false or misleading and constitute[d] a deceptive act or practice").

[28] 15 U.S.C. § 45(n).

[29] *Id.* at 6 ("[R]espondent's failure to employ reasonable and appropriate measures to protect consumer information . . . was, and is, an unfair act or practice.").

[30] *See generally* Bureau of Consumer Protection, *Legal Resources*, BUSINESS.FTC.GOV, http://business.ftc.gov/legal-resources/48/35 (last visited June 29, 2012) (listing recent Federal Trade Commission enforcement of privacy laws).

According to recent consumer privacy guidelines from the Federal Trade Commission, even aggregated non-PII data must be protected, because recent technological advances have allowed companies to combine disparate pieces of non-PII data in a manner that can lead to identification of a particular consumer or device.[31] The implication is that even aggregated, non-PII data may be considered reasonably linkable to an individual.[32] Under the final version of the Federal Trade Commission Privacy Framework, "a company's data would not be [deemed] reasonably linkable to a particular customer or device to the extent that the company implements three significant protections for that data."[33] First, "the company must take reasonable measures to ensure that the data is de-identified. This means that the data cannot reasonably be used to infer information about, or otherwise be linked to, a particular consumer, computer, or other device."[34] Second, "a company must publicly commit to maintain and use the data in a de-identified fashion, and not to attempt to re-identify the data."[35] Finally, "if a company makes such de-identified data available to other companies – whether service providers or other third parties – it should contractually prohibit such entities from attempting to re-identify the data."[36]

C. Privacy Risks and Children

The Federal Trade Commission views protecting children as one of its core missions.[37] In a recent Staff Report, the Federal Trade Commission indicated its continued focus on protecting children's privacy under the authority of the Children's Online Privacy Protection Act

[31] FEDERAL TRADE COMMISSION, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE, *supra* note 15, at 20.

[32] *Id.*

[33] *Id.* at 20-21.

[34] *Id.*

[35] *Id.*

[36] *Id.*

[37] FEDERAL TRADE COMMISSION, MOBILE APPS FOR KIDS: CURRENT PRIVACY DISCLOSURES ARE DISAPPOINTING (2012), *available at* http://www.ftc.gov/os/2012/02/120216mobile_apps_kids.pdf.

("COPPA"), particularly with respect to mobile applications.[38] COPPA, and the Federal Trade Commission Rule that implements it, regulates the online collection of personal information from children under the age of thirteen.[39] In recent years, COPPA has become a major source of legal liability for website and mobile application operators as the Federal Trade Commission has acted to enforce compliance with its provisions.[40] Although COPPA may apply to operators of websites on any platform, it is of particular importance for operators of mobile applications and websites with social components due to their increasing popularity with young children.[41]

COPPA applies to (1) operators of commercial websites or online services (including mobile applications)[42] directed to children and that collect personal information from children, and (2) operators of general audience websites or online services that have *actual knowledge* that they are collecting personal information from children.[43] "[A] Web site operator is considered to have actual knowledge if the site asks for – and receives – information from the user from which age can be determined.[44] To determine whether a Web site is directed to children,

> the FTC considers several factors, including the subject matter; video or audio content; the age of the models on the site; language;

---

[38] *Id* at 1-2.

[39] FEDERAL TRADE COMMISSION, HOW TO COMPLY WITH THE CHILDREN'S ONLINE PRIVACY PROTECTION RULE: A GUIDE FROM THE FEDERAL TRADE COMMISSION, THE DIRECT MARKETING ASSOCIATION, AND THE INTERNET ALLIANCE 1 (2006).

[40] *See, e.g.*, United States v. W3 Innovations, LLC, No. CV-11-03958 (N.D. Cal. Sept. 9, 2011) (consent decree) (ordering the defendant, a mobile app developer, to pay a civil penalty of $50,000 for violations of COPPA); United States v. Playdom, Inc., No. SACV-11-0724-AG (ANx) (C.D. Cal. May 24, 2011) (consent decree) (ordering the defendant, a website operator, to pay a civil penalty of $3,000,000 for violations of COPPA).

[41] *See* FEDERAL TRADE COMMISSION, MOBILE APPS FOR KIDS, *supra* note 29, at 2, 5-9.

[42] Children's Online Privacy Protection Rule, 76 Fed. Reg. 59,804 (proposed Sept. 27, 2011) (stating that "online services" currently covered by the COPPA Rule "includes mobile applications that allow children to play network-connected games, engage in social networking activities, purchase goods or services online, receive behaviorally targeted advertisements, or interact with other content or services."), *available at* http://www.gpo.gov/fdsys/pkg/FR-2011-09-27/pdf/2011-24314.pdf.

[43] 15 U.S.C.A. § 6502(a)(1) (West 2012).

[44] OFFICE OF CONSUMER AND BUSINESS EDUCATION, FEDERAL TRADE COMMISSION, THE CHILDREN'S ONLINE PRIVACY PROTECTION RULE: NOT JUST FOR KIDS' SITES 1 (2004).

> whether advertising on the Web site is directed to children; information regarding the age of the actual or intended audience; and whether a site uses animated characters or other child-oriented features.[45]

If a company operates a website that falls within one of these categories and collects information that is "personal" under the terms of COPPA,[46] it is subject to several obligations. First, operators must "provide notice on the website of what information is collected from children by the operator, how the operator uses such information, and the operator's disclosure practices for such information."[47] Second, operators must make reasonable efforts to "obtain verifiable parental consent for the collection, use, or disclosure of personal information from children."[48] "Verifiable parental consent" is defined as

> any reasonable effort (taking into consideration available technology), including a request for authorization for future collection, use, and disclosure described in the notice, to ensure that a parent of a child receives notice of the operator's personal information collection, use, and disclosure practices, and authorizes the collection, use, and disclosure, as applicable, of personal information and the subsequent use of that information before that information is collected from that child.[49]

Third, the regulations require operators to provide parents with a description of the types of information collected from their children, the opportunity to refuse to permit the operator's further use or maintenance of that information, and a means for parents to obtain any personal information collected from their children.[50] Fourth, operators are prohibited from "conditioning a child's participation in a game, the offering of a prize, or another activity on the child disclosing

---

[45] *See* FEDERAL TRADE COMMISSION, HOW TO COMPLY WITH COPPA, *supra* note 29, at 1.

[46] *See* 15 U.S.C.A. § 6501 (defining the term "personal information" to include personally identifiable information such as a person's first and last name, physical address, e-mail address, telephone number, Social Security number, and other data that could permit the physical or online contacting of a specific individual).

[47] 15 U.S.C. § 6502(b)(1)(A)(i).

[48] 15 U.S.C. § 6502(b)(1)(A)(ii).

[49] 15 U.S.C. § 6501(9).

[50] 15 U.S.C. § 6502(b)(1)(B).

more personal information than is reasonably necessary to participate in such activity."[51] Finally, operators are required to "establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children."[52]

Clearly, COPPA imposes a potentially onerous burden on companies that collect children's personal information via social media or mobile applications. Given the breadth of the restrictions and the Federal Trade Commission's stated intention to step up enforcement efforts,[53] corporate counsel should be vigilant in order to avoid potential pitfalls.

D. Industry-Specific Privacy Issues: Financial Services, Health Care, and Education

In addition to general privacy regulations under the Federal Trade Commission Act and the Children's Online Privacy Protection Act, there are a number of industry-specific obligations that may create potential legal liabilities for companies based on the information they collect, maintain, and use. In particular, healthcare providers and financial services companies may be subject to additional, content-specific regulations.

For example, the Health Insurance Portability and Accountability Act and the administrative rules that implement it (HIPAA) protect health information "that identifies the individual" or "with respect to which there is a reasonable basis to believe the information can be used to identify the individual."[54] HIPAA's Privacy Rule applies to health care providers, health plans, and health care clearinghouses.[55]

---

[51] 15 U.S.C. § 6502(b)(1)(C).

[52] 15 U.S.C. § 6502(b)(1)(D).

[53] *See* FEDERAL TRADE COMMISSION, MOBILE APPS FOR KIDS, *supra* note 29, at 2, 17 ("Over the next six months, staff will conduct an additional review [of companies' privacy practice with respect to mobile applications] to determine whether there are COPPA violations and whether enforcement is appropriate. . . . Staff is committed to working with all stakeholders on these issues, and also plans to continue its vigorous enforcement of the COPPA statute and Rule.")

[54] HIPAA Privacy Rule, 45 C.F.R. § 160.103 (2012).

[55] *Id.*

Similarly, laws related to consumer financial privacy and security affect companies that deal with consumers' personal information. For example, the Gramm-Leach-Bliley Financial Modernization Act of 1999 requires financial institutions "to give consumers privacy notices that explain the institutions' information-sharing practices. In turn, consumers have the right to limit some – but not all – sharing of their information."[56] The Act defines "financial institutions" as "any institution engaged in the business of providing financial services to customers who maintain a credit, deposit, trust, or other financial account or relationship with the institution" (subject to a number of exceptions).[57] The definition of protected information is also broad, covering all "customer information of a financial institution," which includes "any information maintained by or for a financial institution which is derived from the relationship between the financial institution and a customer of the financial institution and is identified with the customer."[58]

These examples are by no means exhaustive but are intended to demonstrate that, in addition to the general privacy protections imposed by the Federal Trade Commission pursuant to their authority under the Federal Trade Commission Act, there may be industry-specific safeguards that impose obligations on certain companies. For these companies, obligations imposed by industry-specific laws would apply equally in the social media and mobile contexts.

E. Advertising and Social Media: Endorsements

Potential legal liabilities related to advertising through new media are not limited to privacy issues. The proliferation of social media platforms such as Facebook and Twitter, coupled with increased access to internet platforms due to the ubiquity of internet-capable

[56] FEDERAL TRADE COMMISSION, IN BRIEF: THE FINANCIAL PRIVACY REQUIREMENTS OF THE GRAMM-LEACH-BLILEY ACT 1 (2002).

[57] Gramm-Leach-Bliley Act, 15 U.S.C. § 6827(4).

[58] Gramm-Leach-Bliley Act, 15 U.S.C. § 6827(2).

mobile devices such as smartphones and tablets has made it trivially easy for consumers to review and comment on the products and services they encounter. In many cases, a customer's approval can be noted and published at the click of a button (e.g., the Google "+1" button, Facebook "like" and "share" buttons, and Twitter button). The mark of approval can be valuable. According to a recent New York Times article, Facebook has told investors that "consumers were 50 percent more likely to recall an ad if it came with a plug from a Facebook friend."[59] For celebrities, social media status has become a key factor in securing endorsement deals.[60]

Companies should be aware that comments about their products on social media platforms may be considered endorsements or testimonials, and that the Federal Trade Commission has actively sought to prevent deceptive endorsement practices. The National Advertising Division (NAD) of the Council of Better Business Bureaus has also been active in this area. The NAD provides a self-regulatory mechanism for the advertising industry and serves to resolve disputes about factual claims in advertising through a process of alternative dispute resolution administered by the Council of Better Business Bureaus.[61] The Federal Trade Commission defines an endorsement as

> any advertising message . . . that consumers are likely to believe reflects the opinions, beliefs, findings, or experiences of a party other than the sponsoring advertiser, even if the views expressed by that party are identical to those of the sponsoring advertiser.[62]

In 2009, in response to the changing media and advertising landscape, the Federal Trade Commission issued revised guidelines for the use of testimonials and endorsements in

[59] Somini Senguptam, *On Facebook, 'Likes' Become Ads*, N.Y. TIMES, May 31, 2012, at A1, *available at* http://www.nytimes.com/2012/06/01/technology/so-much-for-sharing-his-like.html?pagewanted=all.

[60] *See* Andrew Hampp, *Social Media Status Key to Endorsements for Today's Celeb*, AD AGE MEDIA NEWS (Sept. 19, 2011), http://adage.com/article/media/social-media-status-key-endorsements-today-s-celeb/229843.

[61] *See generally*, About NAD, ASRC, http://www.asrcreviews.org/about-us (last visited July 18, 2012).

[62] 16 C.F.R. § 255.0(b).

advertising.[63] The revised endorsement guides reflect three basic principles. First, "[e]ndorsements must be truthful and not misleading."[64] Second, "[i]f the advertiser doesn't have proof that the endorser's experience represents what consumers will achieve by using the product, the ad must clearly and conspicuously disclose the generally expected results in the depicted circumstances."[65] Third, "[i]f there's a connection between the endorser and the marketer of the product that would affect how people evaluate the endorsement, it should be disclosed."[66] Each of the specific regulations reflects these guiding principles.

Many forms of endorsements subject to disclosure and substantiation requirements existed long before the advent of social media. For example, when an expert or celebrity makes a claim about a product, that claim must reflect "the honest opinions, findings, beliefs, or experience of the endorser . . . and may not convey any express or implied representation that would be deceptive if made by the advertiser."[67] Moreover, if the endorser is an expert, her "qualifications must in fact give [her] the expertise that [she] is represented as possessing with respect to the endorsement."[68] More generally, whenever "there exists a connection between the endorser and the seller of the advertised product that might *materially affect the weight or credibility of the endorsement* (*i.e.*, the connection is not reasonably expected by the audience), such connection must be fully disclosed."[69]

---

[63] Guides Concerning the Use of Endorsements and Testimonials in Advertising, 16 C.F.R. § 255 (2012).

[64] FEDERAL TRADE COMMISSION, THE FTC'S REVISED ENDORSEMENT GUIDES: WHAT PEOPLE ARE ASKING 1 (2010), *available at* http://business.ftc.gov/documents/bus71-ftcs-revised-endorsement-guideswhat-people-are-asking.

[65] *Id.*

[66] *Id.*

[67] 16 C.F.R. § 255.1(a).

[68] 16 C.F.R. § 255.3(a).

[69] 16 C.F.R. § 255.5 (emphasis added).

What may be less apparent are the ways in which the new media landscape has given rise to new potential legal liabilities as it has expanded opportunities for consumers and customers to interact through social media. Many of these potential pitfalls arise in the context of consumer endorsements and relate to disclosure of material connections between the endorser and the company, disclaimers regarding typicality of experience, or the substantiation of claims made by the endorser.[70] For example, the Federal Trade Commission brought charges against the public relations agency Reverb Communications, Inc. in 2010,[71] alleging that it "engaged in deceptive advertising by having employees pose as ordinary consumers posting game reviews at the online iTunes store, and not disclosing that the reviews came from paid employees working on behalf of the developers."[72] Reverb settled the charges.[73] Even when an endorser does not receive payment in exchange for writing a review of a product (e.g., on a blog or through Facebook, Twitter, or LinkedIn), there may be a disclosure requirement if that individual has received free products or services from the endorsed company[74] or is an employee of that company.[75] Following its

[70] *See* 16 C.F.R. § 255.2 (describing substantiation and typicality of experience requirements for consumer endorsements); 16 C.F.R § 255.5 (describing disclosure requirements for material connections between the endorser and the company).

[71] Complaint, *In re* Reverb Communications, Inc., No. 092-3199, 2010 WL 3441879 (F.T.C. Aug. 26, 2010).

[72] Federal Trade Commission, *Public Relations Firm to Settle FTC Charges that It Advertised Clients' Gaming Apps Through Misleading Online Endorsements*, FTC.GOV (Aug. 26, 2010), http://www.ftc.gov/opa/2010/08/reverb.shtm.

[73] *Id.*

[74] *See, e.g.*, 16 C.F.R. § 255.5 Example 8 ("An online message board designated for discussion of new music download technology is frequented by MP3 player enthusiasts. They exchange information about new products, utilities, and the functionality of numerous playback devices. Unbeknownst to the message board community, an employee of a leading playback device manufacturer has been posting messages on the discussion board promoting the manufacturer's product. Knowledge of this poster's employment likely would affect the weight or credibility of her endorsement. Therefore, the poster should clearly and conspicuously disclose her relationship to the manufacturer to members and readers of the message board.")

[75] *See, e.g.*, 16 C.F.R. § 255.5 Example 7 ("A college student who has earned a reputation as a video game expert maintains a personal weblog or 'blog' where he posts entries about his gaming experiences. Readers of his blog frequently seek his opinions about video game hardware and software. As it has done in the past, the manufacturer of a newly released video game system sends the student a free copy of the system and asks him to write about it on his blog. He tests the new gaming system and writes a favorable review. Because his review is disseminated via a form of consumer-generated media in which his relationship to the advertiser is not inherently obvious, readers are unlikely to know that he has received the video game system free of charge in exchange for his review of the

guidelines, the Federal Trade Commission closely scrutinizes any relationship that might materially affect the credibility of a consumer-generated endorsement.

However, the law is still developing with respect to relationships that are more tenuous than those described in the preceding examples. For example, the FTC and NAD are beginning to consider the question of whether Facebook "likes" or Twitter "retweets" constitute consumer endorsements. The NAD recently held that "[t]he display of likes on Facebook and other social platforms may reasonably be understood by consumers as conveying a message of general social endorsement.[76] It also cautioned that it may require a company to remove "likes" if the advertiser used misleading or artificial means to inflate the number of Facebook "likes."[77]

III. Employment Issues

Social media and ubiquitous access to the Internet have allowed people to extensively document their day-to-day lives and, in many cases, to publish that (sometimes trivial) information to be viewed by their friends and followers.[78] For employers, this is a potential resource as well as a cause for concern. As part of the hiring process, extensive information about potential employees' personal and professional lives may provide a valuable tool for

---

product, and given the value of the video game system, this fact likely would materially affect the credibility they attach to his endorsement. Accordingly, the blogger should clearly and conspicuously disclose that he received the gaming system free of charge. The manufacturer should advise him at the time it provides the gaming system that this connection should be disclosed, and it should have procedures in place to try to monitor his postings for compliance."

[76] Coastal Contacts, Inc., Case No. 5387, NAD/CARU Case Reports (Oct. 2011), *available at* http://www.narcpartners.org/reports/CaseReports.aspx.

[77] *Id.* at 17-18.

[78] *See, e.g.,* Roger Kay, *The Unbearable Triviality of Social Networking*, FORBES (April 18, 2011, 10:44 AM), http://www.forbes.com/sites/rogerkay/2011/04/18/the-unbearable-triviality-of-social-networking ("Social networking is not new. Before Twitter, we had Facebook, and before that, News Corp's MySpace, and before that, AOL, and before that, local bulletin boards like the Well, and before that, the local bar. But what began as a demonstration of 'meta-reailty' or making a difference in each other's lives even when we were not actually present, has become a blather-fest, everybody talking, nobody listening.").

employers.[79] At the same time, employees have used social media to complain about working conditions or to disclose sensitive or proprietary information, giving rise to the question of when it is appropriate to terminate an employee based on social media postings.[80] Over the past few years, the National Labor Relations Board has begun to scrutinize the social media policies that companies are using to make these hiring and firing decisions.

The National Labor Relations Board (NLRB) is the federal agency tasked with investigating instances of unfair labor practices committed by private-sector employers and unions.[81] The NLRB's enforcement authority in this capacity is derived from the National Labor Relations Act (NLRA).[82] Section 7 of the NLRA gives employees the right to form, join, or assist labor organizations and to engage in other concerted activities for the purpose of collective bargaining or other mutual aid or protection.[83] Even in the absence of a labor union, an employee complaining about wages, hours, or working conditions on behalf of herself and other employees cannot be disciplined or discharged for such conduct.[84] It is considered an unfair labor practice for an employer to "interfere with, restrain, or coerce employees in the exercise of the rights guaranteed in section 7 [of the NLRA]."[85] Applying this provision to an employer's social media policy, the NLRB has stated that

---

[79] *See, e.g.*, Jennifer Preston, *Social Media History Becomes a New Job Hurdle*, N.Y. TIMES, July 20, 2011, at B1, *available at* http://www.nytimes.com/2011/07/21/technology/social-media-hitory-becomes-a-new-job-hurdle.html?pagewanted=all; Lisa Quast, *How Your Social Media Profile Could Make or Break Your Next Job Opportunity*, Forbes (April 23, 2012, 9:11 AM), http://www.forbes.com/sites/lisaquast/2012/04/23/your-social-media-profile-could-make-or-break-your-next-job-opportunity.

[80] *See* Melanie Trottman, *For Angry Employees, Legal Cover for Rants*, The Wall Street Journal (Dec. 2, 2011), http://online.wsj.com/article/SB10001424052970203710704577049822809710332.html.

[81] *See* National Labor Relations Board, *What We Do*, NLRB.GOV, http://www.nlrb.gov/what-we-do (last visited July 19, 2012).

[82] 29 U.S.C. §§151-169 (2012).

[83] 29 U.S.C. § 157.

[84] *Id.*

[85] 29 U.S.C. § 158(a)(1).

> [a]n employer violates Section 8(a)(1) of the Act through the maintenance of a work rule if that rule would reasonably tend to chill employees in the exercise of their Section 7 rights. The Board uses a two-step inquiry to determine if a work rule would have such an effect. First, a rule is unlawful if it explicitly restricts Section 7 activities. If the rule does not explicitly restrict protected activities, it is unlawful only upon a showing that: (1) employees would reasonably construe the language to prohibit Section 7 activity; (2) the rule was promulgated in response to union activity; or (3) the rule has been applied to restrict the exercise of Section 7 rights.[86]

In a series of recent reports, the NLRB has used this standard to evaluate the legality of employers' social media policies, in many cases finding that the policies unlawfully restricted protected Section 7 activity in a variety of contexts.[87] A perusal of the report's findings demonstrates the NLRB's willingness to find fault with even innocuous-sounding provisions.

Policies that attempt to protect confidential information may be interpreted to impermissibly restrict protected Section 7 activity.[88] For example, a privacy policy that prohibited the "release of confidential guest, team member, or company information" was considered unlawful because it would "reasonably be interpreted as prohibiting employees from discussing and disclosing information regarding their own conditions of employment, as well as the conditions of employment of employees other than themselves—activities that are clearly protected under Section 7."[89] Similarly, a policy that required employees to obtain permission from the employer before speaking to the media (including posting on blogs, etc.) was

---

[86] OFFICE OF THE GENERAL COUNSEL, NATIONAL LABOR RELATIONS BOARD, OM 11-74, REPORT OF THE ACTING GENERAL COUNSEL CONCERNING SOCIAL MEDIA CASES WITHIN THE LAST YEAR (2011) (internal citations and quotations omitted).

[87] *See generally*, OFFICE OF THE GENERAL COUNSEL, NATIONAL LABOR RELATIONS BOARD, OM 12-59, REPORT OF THE ACTING GENERAL COUNSEL CONCERNING SOCIAL MEDIA CASES (2012); OFFICE OF THE GENERAL COUNSEL, NATIONAL LABOR RELATIONS BOARD, OM 12-31, REPORT OF THE ACTING GENERAL COUNSEL CONCERNING SOCIAL MEDIA CASES (2012); OFFICE OF THE GENERAL COUNSEL, NATIONAL LABOR RELATIONS BOARD, OM 11-74, REPORT OF THE ACTING GENERAL COUNSEL CONCERNING SOCIAL MEDIA CASES WITHIN THE LAST YEAR (2011).

[88] *See* OFFICE OF THE GENERAL COUNSEL, NATIONAL LABOR RELATIONS BOARD, OM 12-59, REPORT OF THE ACTING GENERAL COUNSEL CONCERNING SOCIAL MEDIA CASES 4-5, 7, 12 (2012).

[89] *Id.* at 4.

considered impermissible.[90] According to the report, "[e]mployees have a protected right to seek help from third parties regarding their working conditions. This would include going to the press, blogging, speaking at a union rally, etc."[91]

Social media policies designed to keep employees from discussing sensitive or controversial topics may also be considered overbroad. The Office of the General Counsel reported that a policy admonishing employees to "treat everyone with respect" and stating that "offensive, demeaning, abusive or inappropriate remarks are as out of place online as they are offline" was unlawful because it "proscribe[d] a broad spectrum of communications that would include protected criticisms of the Employer's labor policies or treatment of employees."[92] Provisions instructing employees to "[a]dopt a friendly tone when engaging online," to not "pick fights," and to "[t]hink carefully about 'friending' coworkers . . . on social media sites" were similarly found to be unlawful.[93]

Importantly, the report made it clear that a social media policy's statement "[would] not be construed or applied in a manner that improperly interferes with employees' rights under the National Labor Relations Act" did not insulate the employer from liability for the "otherwise unlawful provisions of [its] social media policy because employees would not understand from this disclaimer that protected activities are in fact permitted."[94] In contrast, the report recognized that certain specific provisions, such as those prohibiting "harassment, bullying, discrimination,

[90] *Id.* at 17-18.

[91] *Id.* at 18.

[92] *Id.* at 8.

[93] *Id.* at 8, 10.

[94] *Id.* at 12.

or retaliation that would not be permissible in the workplace," were lawful. It also reproduced an example of a complete social media policy that was considered to be lawful in its entirety.[95]

The implication for employers is that the NLRB has taken a serious and focused interest in social media policies, and that many provisions of these policies may be considered illegal under the terms of the NLRA. It is important for companies to review these policies to ensure that they are protected from liability.

IV. Liability for the Actions of Users: The Communications Decency Act

It is common for websites and mobile applications to allow users to post content. It is important for companies to understand the circumstances in which they are or are not liable for third-party content, which can in some cases be offensive or even tortious. Enacted in 1996, the Communications Decency Act provides broad immunity for companies that allow third-party content.[96] Under the Act, "[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."[97] Moreover,

> No provider or user of an interactive computer service shall be held liable on account of any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or any action taken to enable or make available to information content providers or others the technical means to restrict access to [such material].[98]

[95] *Id.* at 22-24.

[96] 47 U.S.C. § 230 (2012).

[97] *Id.* at § 230(c)(1).

[98] *Id.* at § 230(c)(2).

Under the terms of the Act, an "information content provider" is defined 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."[99]

In most cases, the Act insulates service providers from liability for defamation and other causes of action based on content posted by third parties. A recent article in the American Bar Association journal *Communications Lawyer* neatly summarizes the protection afforded by the Communications Decency Act:

> Section 230 provides broad protection for neutral actions that media entities and other interactive computer services might take concerning third-party content posted on their websites. Hosting, reviewing, editing, and even soliciting content all typically are protected activities so long as the media entity does not create or solicit the offensive portion of the third-party submission.[100]

Courts have not applied this immunity without limitation, however, and it is important to recognize the Act's limitations:

> Case law indicates . . . that CDA protection may be lost when (1) the media entity promises to remove the offensive content and fails to do so; (2) the posting is made pursuant to an authorized agency or employment relationship with the media entity; (3) the media entity engages in conduct that is unlawful apart from the publication of the content; (4) the media entity inserts the offensive content; or (5) the media entity solicits the offensive portion of the third-party submission.[101]

A pair of recent cases illustrate how the Communications Decency Act is applied in practice, both to the benefit and detriment of companies that host third-party content.

---

[99] *Id.* at § 230(f)(3).

[100] Edward Fenno & Christina Humphries, *Protection Under CDA § 230 and Responsibility for "Development" of Third-Party Content*, COMMUNICATIONS LAWYER, Aug. 2011, at 33.

[101] *Id.*

Hill v. StubHub, Inc. provides an example of Section 230 being applied to insulate a company from liability.[102] Stubhub, Inc. is an "online marketplace that enables third parties to buy and sell tickets to sporting contests, concerts, and similar events[, serving] as an intermediary between buyers and sellers in order to facilitate transactions."[103] In *Hill*, the plaintiffs claimed that Stubhub had violated a North Carolina statute "making it unlawful to sell a ticket for more than $3.00 over its face value" and by engaging in unfair and deceptive trade practices.[104] The trial court granted summary judgment in favor of the plaintiffs, holding that Stubhub's conduct constituted an unfair and deceptive practice and that it was not entitled to immunity under Section 230.[105] The defendant appealed, and the Court of Appeals of North Carolina reversed, holding that 47 U.S.C. § 230 did in fact immunize Stubhub against the state law claims.[106] After a discussion of the limited situations in which the Act had been held not to provide immunity for claims based on third-party content, the court stated that "[a]ccording to [its] research, there have been approximately 300 reported decisions addressing immunity claims advanced under 47 U.S.C. § 230 in the lower federal and state courts," and that "[a]ll but a handful of these decisions find that the website is entitled to immunity from liability."[107] In finding Stubhub immune under the Act, the court held that

> in order to lose the benefit of the exemption from liability granted by 47 U.S.C. § 230 based upon content actually posted by third parties, an analysis of the results reached in persuasive decisions from other jurisdictions establishes that, in order to 'materially contribute' to the creation of unlawful material, a website must effectively control the content posted by those third parties or take

[102] No. COA11-685, 2012 WL 696223 (N.C. Ct. App. Mar. 6, 2012).

[103] *Id.* at *1.

[104] *Id.* at *2.

[105] *Id.* at *3.

[106] *Id.* at *1.

[107] *Id.* at *9.

> other actions which essentially ensure the creation of unlawful material.[108]

This case is typical of Section 230 jurisprudence in situations where the defendant has not taken an active role in controlling or promoting the third-party creation and posting of unlawful material. However, when a company takes a more active role with respect to actionable content, it may lose the immunity it would normally enjoy under the Act.

Jones v. Dirty World Entm't Recordings, LLC is a recent example of this latter situation.[109] In *Jones*, the plaintiff, a high school teacher and member of the Cincinnati Bengals' cheerleading squad, brought a defamation and invasion of privacy action against the operator of an Internet site known as "thedirty.com" and the corporations through which he operated it.[110] The defendants moved for judgment as a matter of law, claiming absolute immunity under the Communications Decency Act.[111] After noting that "[t]his grant of immunity applies only if the interactive computer service provider is not also an 'information content provider,' which is defined as someone who is '*responsible, in whole or in part, for the creation or development* of' the offending content,"[112] the court reviewed the relevant case law to identify an appropriate test for determining whether actions by a web site operator constitute creation or development of offending content.[113] It adopted the test applied by the 10th Circuit in *Federal Trade Comm'n v. Accusearch, Inc.*, which held that "a service provider is "responsible" for the development of

[108] *Id.* at *13.

[109] No. 09-219-WOB, 2012 WL 70426 (E.D. Ky. Jan. 10, 2012).

[110] *Id.* at *1.

[111] *Id.*

[112] *Id.* at *2 (citing 47 U.S.C. § 230(f)(3)) (emphasis in original).

[113] *Id.* at*2-3.

offensive content only if it in some way specifically encourages the development of *what is offensive about the content*."[114]

Applied to the facts at hand, the court held that the defendants were not entitled to immunity under the Communications Decency Act.[115] This decision was based on the fact that the very name of the site ("thedirty.com") itself "encourage[d] the posting only of . . . material which is potentially defamatory or an invasion of the subject's privacy," the operator of the website specifically solicited and encouraged offensive content through a link to "submit dirt," and the fact that the operator frequently added his own comments to postings.[116]

V. Intellectual Property and the Digital Millennium Copyright Act

While the Communications Decency Act protects companies from liability for the third-party content of their users, it also states that "nothing in this section shall be construed to limit or expand any law pertaining to intellectual property."[117] Content posted by third parties is not limited to blog postings or comments on message boards, however, and includes a variety of media, including video and audio files that may be subject to copyright protections. The Digital Millennium Copyright Act (DMCA) of 1998,[118] signed into law by President Clinton, addresses this problem by, among other things, "create[d] new limitations on liability for copyright infringement by online service providers."[119] As social media and the sharing of content have

[114] *Id.* at *3, *quoting* 570 F.3d 1187 (10th Cir. 2009).

[115] *Id.* at *5.

[116] One example of a post concerning the plaintiff was "Why are all high school teachers freaks in the sack?" *Id.* at *4.

[117] 47 U.S.C. § 230(e)(2).

[118] Pub. L. No. 104-304, 112 Stat. 2860 (Oct. 28, 1998).

[119] Online Copyright Infringement Liability Limitation, 17 U.S.C. § 512 (2012).

accelerated rapidly[120] over the past decade, the DMCA has largely protected websites from infringement by third parties through a provision known as the Safe Harbor Rule.[121] Like the Communications Decency Act, however, there are limitations on this immunity, and businesses that allow third-party users to upload content using social media and mobile devices must be careful to avoid liability for their users' copyright infringement. Mistakes can be serious.

In a highly public example from January 2012, federal authorities shut down Megaupload.com and charged its founder, Kim Dotcom, with criminal copyright infringement money laundering, and conspiracy to commit racketeering.[122] The indictment alleged that "[s]ince at least September 2005, Megaupload.com has been used by the defendants . . . to willfully reproduce and distribute millions of infringing copies of copyrighted works, including motion pictures, television programs, musical recordings, electronic books, images, video games, and other computer software."[123] Dotcom was arrested at his home in New Zealand and is currently awaiting an extradition hearing scheduled for March 2013.[124] While the Megaupload case may be a unique example of alleged copyright infringement based on third-party content, courts over the last few years have been working to define the limits of the DMCA's exemptions.

Title II of the DMCA provides four "safe harbors" that insulate certain service providers from copyright infringement liability based on (a) "transitory digital network communications,"

---

[120] For example, 72 hours of video are uploaded to YouTube, the popular video sharing site, every minute. Three hours of video is uploaded every minute to YouTube from mobile devices. *Statistics*, YOUTUBE.COM, http://www.youtube.com/t/press_statistics (last visited July 20, 2012).

[121] 17 U.S.C. § 512.

[122] Geoffrey A. Fowler, Devlin Barrett & Sam Schechner, *U.S. Shuts Offshore File-Share 'Locker'*, THE WALL STREET JOURNAL (Jan. 20, 2012), http://online.wsj.com/article/SB 10001424052970204616504577171060611948408.html.

[123] Superseding Indictment, U.S. v. Dotcom, No. 1:12CR3 (E.D. Va filed Feb. 16, 2012).

[124] Joe Schneider, *U.S. Bid for Megaupload Founder Dotcom's Extradition is Delayed*, BLOOMBERG (July 9, 2012, 10:35 PM), http://www.bloomberg.com/news/2012-07-10/u-s-bid-for-megaupload-founder-dotcom-s-extradition-is-delayed.html.

(b) "system caching," (c) "information residing on systems or networks at [the] direction of users," and (d) "information location tools."[125] In order to qualify for any of these safe harbors, a

> party must in fact be a "service provider," defined in pertinent part, as "a provider of online services or network access, or the operator of facilities therefore." A party that qualifies as a service provider must also satisfy certain "conditions of eligibility," including the adoption and reasonable implementation of a "repeat infringer" policy that "provides for the termination in appropriate circumstances of subscribers and account holders of the service provider's system or network." In addition, a qualifying service provider must accommodate "standard technical measures" that are "used by copyright owners to identify or protect copyrighted works."[126]

In addition to the general criteria set forth in Title II of the Act, a service provider is required to meet certain additional requirements of the specific safe harbor it is trying to invoke. The safe harbor for "information residing on systems or networks at [the] direction of users" has been particularly important for social media and mobile platforms that allow users to post content.

A service provider only qualifies for this safe harbor if it

> (A) (i) does not have actual knowledge that the material or an activity using the material on the system or network is infringing; (ii) in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent; or (iii) upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material;
>
> (B) does not receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity; and
>
> (C) upon notification of claimed infringement . . . responds expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity.[127]

---

[125] 17 U.S.C. § 512(a)-(d).

[126] Viacom Int'l., Inc. v. YouTube, Inc., 676 F.3d 19, 27 (2d Cir. 2012) (internal citations omitted).

[127] 17 U.S.C. § 512(c)(1)(A)-(C).

Finally, the Act sets forth a detailed notification scheme that requires service providers to "designate an agent to receive notification of claimed infringement"[128] and "defines the components of a proper notification, commonly known as a 'takedown notice.'"[129]

The most important recent case law in this area has focused on the level of knowledge that would cause a service provider to lose immunity under the statute. The United States Court of Appeals for the Second Circuit is the latest court to issue an important ruling defining the scope of protections under the DMCA's safe harbor provisions.[130] In *Viacom Int'l, Inc. v. YouTube, Inc.*, the Second Circuit upheld the District Court's ruling that the phrases "actual knowledge that the material is infringing"[131] and "facts or circumstances from which infringing activity is apparent"[132] refer to "knowledge of specific and identifiable infringements."[133] This means that, "actual knowledge or awareness of facts or circumstances that indicate specific and identifiable instances of infringement will disqualify a service provider from the safe harbor."[134] The Court explicitly rejected an alternative construction of the statute, which would have interpreted the provision to mean that a service provider would lose protection if it had actual knowledge or constructive knowledge that infringements were occurring, even when it did not or could not identify specific instances of infringement.[135] In response to the plaintiffs' claims that the defendants were "willfully blind" to specific infringing activity, the court held that "DMCA safe harbor protection cannot be conditioned on affirmative monitoring by a service provider,"

[128] *Id.* at § 512(c)(2).

[129] 676 F.3d at 27 (citing 17 U.S.C. § 512(c)(3)).

[130] 67 F.3d 19.

[131] 17 U.S.C. § 512(c)(1)(A).

[132] *Id.*

[133] 676 F.3d at 30 (quoting *Viacom Int'l, Inc. v. YouTube, Inc.*, 718 F. Supp. 2d 514, 523 (S.D.N.Y. 2010)).

[134] *Id.*at 32.

[135] *Id.* at 31-32.

but that "the willful blindness doctrine may be applied, in appropriate circumstances, to demonstrate knowledge or awareness of specific instances of infringement under the DMCA."[136] Having made these determinations, the Circuit Court vacated the District Court's order of summary judgment in favor of the defendants and remanded the case to resolve a number of material factual issues, including whether or not YouTube had actual knowledge of specific instances of infringement.[137]

Companies that allow users to post content are closely monitoring the outcome of the *Viacom* case and are adjusting their copyright policies to fit the reality that the DMCA's protections are not limitless. For example, Pinterest, a popular social networking site that allows users to post and share content,[138] recently updated its copyright and trademark policies in response to concern over whether or not it was protected by the DMCA's safe harbor provisions.[139]

VI. Conclusion

The new media landscape is rapidly changing, and both companies and the government have been forced to make rapid adjustments to their policies. Companies must recognize that their interactions with a highly social and mobile population are subject to a complex and evolving body of laws. As consumers, companies, employees, and the government interact in an increasingly interconnected business environment, avoiding legal pitfalls will require all parties to adapt.

---

[136] *Id.* at 35.

[137] *Id.* at 26.

[138] *See* http://pinterest.com (last visited July 20, 2012).

[139] Hayley Tsukayama, *Pinterest address copyright concerns*, WASHINGTON POST (Mar. 15, 2012), http://www.washingtonpost.com/business/technology/pinterest-addresses-copyright-concerns/2012/03/15/gIQAijAFES_story.html. *See also*, Pinterest, *Copyright & Trademark*, PINTEREST, http://pinterest.com/about/copyright (last visited July 20, 2012).