LIABILITY OF PLATFORMS

Excerpted from Chapter 49 (The Liability of Platforms (including Website Owners, App Providers, eCommerce Vendors, Cloud Storage and Other Internet and Mobile Service Providers) for User Generated Content and Misconduct) of
E-Commerce and Internet Law: Legal Treatise with Forms 2d Edition
A 5-volume legal treatise by Ian C. Ballon (Thomson/West Publishing, www.IanBallon.net)

GOLDMAN & BALLON ON PLATFORM LIABILITY
GREENBERG TRAURIG, LLP
MAY 2019

Ian C. Ballon
Greenberg Traurig, LLP

Silicon Valley:	Los Angeles:
1900 University Avenue, 5th Fl.	1840 Century Park East, Ste. 1900
East Palo Alto, CA 914303	Los Angeles, CA 90067
Direct Dial: (650) 289-7881	Direct Dial: (310) 586-6575
Direct Fax: (650) 462-7881	Direct Fax: (310) 586-0575

Ballon@gtlaw.com
<www.ianballon.net>
LinkedIn, Twitter, Facebook: IanBallon

This paper has been excerpted from *E-Commerce and Internet Law: Treatise with Forms 2d Edition*
(Thomson West, www.IanBallon.net), the 5-volume legal treatise by Ian C. Ballon

GT GreenbergTraurig

Ian C. Ballon

Shareholder

Internet, Intellectual Property & Technology Litigation

Admitted: California, District of Columbia and Maryland
Second, Third, Fourth, Fifth, Seventh, Ninth, Eleventh and Federal Circuits
U.S. Supreme Court
JD, LLM, CIPP

Ballon@gtlaw.com
LinkedIn, Twitter, Facebook

Silicon Valley
1900 University Avenue
5th Floor
East Palo Alto, CA 94303
T 650.289.7881
F 650.462.7881

Los Angeles
1840 Century Park East
Los Angeles, CA 90067
T 310.586.6575
F 310.586.0575

Ian Ballon is a litigator who is Co-Chair of Greenberg Traurig LLP's Global Intellectual Property & Technology Practice and represents Internet, technology, mobile and other companies in intellectual property and internet- and mobile-related litigation, including defending platforms in DMCA, CDA, fair use, and secondary copyright, trademark and patent infringement suits, as well as defending companies in data privacy, security breach, and TCPA class action suits. He is also the author of the leading treatise on Internet law, *E-Commerce and Internet Law: Treatise with Forms 2d edition,* the 5-volume set published by West (www.IanBallon.net). In addition, he is the author of *The Complete CAN-SPAM Act Handbook* (West 2008) and *The Complete State Security Breach Notification Compliance Handbook* (West 2009). He also serves as Executive Director of Stanford University Law School's Center for E-Commerce, which hosts the annual Best Practices Conference where lawyers, scholars and judges are regularly featured and interact. A list of recent cases may be found at http://www.gtlaw.com/Ian-C-Ballon-experience.

Mr. Ballon was named the Lawyer of the Year for Information Technology Law in the 2019, 2018, 2016 and 2013 editions of Best Lawyers in America. In both 2018 and 2019 he was recognized as one of the Top 1,000 trademark attorneys in the world for his litigation practice by *World Trademark Review*. In addition, in 2019 he was named one of the top 20 Cybersecurity lawyers in California and in 2018 one of the Top Cybersecurity/Artificial Intelligence lawyers in California by the *Los Angeles and San Francisco Daily Journal*. He received the "Trailblazer" Award, Intellectual Property, 2017 from *The National Law Journal* and he has been recognized as a "Groundbreaker" in *The Recorder*'s 2017 Litigation Departments of the Year Awards. In addition, he was the 2010 recipient of the State Bar of California IP Section's Vanguard Award for significant contributions to the development of intellectual property law (http://ipsection.calbar.ca.gov/IntellectualPropertyLaw/IPVanguardAwards.aspx). He is listed in Legal 500 U.S., The Best Lawyers in America (in the areas of information technology and intellectual property) and Chambers and Partners USA Guide in the areas of privacy and data security and information technology. He also has been recognized by *The Daily Journal* as one of the Top 75 IP litigators in California in every year that the list has been published, from 2009 through 2018, and has been listed as a Northern California Super Lawyer every year from 2004 through 2018 and as one of the Top 100 lawyers in California. Mr. Ballon also holds the CIPP/US certification from the International Association of Privacy Professionals (IAPP).

Chapter 49

The Liability of Platforms (including Website Owners, App Providers, eCommerce Vendors, Cloud Storage and Other Internet and Mobile Service Providers) for User Generated Content and Misconduct[1]

[1]This chapter provides a brief overview of secondary liability theories that are analyzed much more extensively in other sections of the treatise, to provide a high level comparison of the liability regimes imposed on intermediaries under different theories of law.

KeyCite®: Cases and other legal materials listed in KeyCite Scope can be researched through the KeyCite service on Westlaw®. Use KeyCite to check citations for form, parallel references, prior and later history, and comprehensive citator information, including citations to other decisions and secondary materials.

49.01 Assessing and Minimizing the Liability Risks from User Content and Conduct—An Overview

Platform providers (including traditional service providers and owners or operators of websites, app providers, eCommerce vendors, cloud storage and other internet and mobile service providers)[1] confront specific secondary (or vicarious)

[Section 49.01]

[1]The terms site owner (or operator) and (more commonly) service provider are used broadly throughout Part IX of the treatise (chapters 48, 49, 50 and 51) to encompass individuals or entities that own or operate locations where user generated content (UGC) or other material may be stored, posted or transmitted by third parties.

The terms *customer* and *subscriber* are used interchangeably to refer to users who have a contractual or other transactional relationship to a site owner or service provider.

Distinctions are not drawn between website owners and operators, or between site owners or operators, on the one hand, and service providers, on the other, all of whom potentially could be subject to third-party (or "secondary" or vicarious) liability for user conduct or content (even though they may have contractual or common law indemnification claims against one another in particular cases).

Additional risks faced by cloud service providers, Internet hosts and storage lockers and mobile services are separately assessed in chapter 50. Special issues involving social networks, blogs, wiki and other Web 2.0 applications are analyzed in chapter 51. The third-party liability risks of domain name registrars and registries (and applicable exemptions) are separately analyzed in section 7.21 (in chapter 7).

All of these entities potentially face liability as intermediaries, which is a term used more commonly in Europe. U.S. law focuses on direct and indirect (or *third-party*) liability. U.S. terminology is further confused by the reference in intellectual property cases to secondary liability as a synonym for indirect or third-party liability. Chapter 48 provides a checklist for direct or primary liability. This chapter focuses on what is variously described as indirect, intermediary, secondary or third-party liability.

The lexicon of terms used to describe various different types of service providers, like the Internet itself, is large and constantly evolving. In the early days of the World Wide Web, distinctions typically were drawn between *content providers*, which made available text, graphics and other content, and *access providers*, which offered connectivity to the Internet. Differentiating between access and content became more difficult by the

liability risks by virtue of their operating a platform, but

---

mid-1990s, when proprietary online services such as America Online, Inc., CompuServe and Prodigy began to offer Internet access. In turn, ISPs—which up until then had been viewed primarily as access providers—began to make available online content and offer subscribers services such as personal homepages. As the line between access and content or service began to blur, an alphabet soup of acronyms emerged, which often were used interchangeably, such as IAP (Internet Access Provider), OAP (Online Access Provider), ISP (Internet Service Provider), OSP (Online Service Provider), ICP (Internet Content Provider) and OCP (Online Content Provider). Terms such as Internet Provider or Online Provider, which omitted any reference to access or service, also came into use.

Through the mid-to late 1990s, when thousands of different ISPs provided Internet access to users—many of which offered hosting and particular, unique services—the distinctions between providers continued to be relevant in assessing liability. As home DSL and cable access grew in popularity, however, connectivity became more commoditized and distinctions between different types of providers became less meaningful in assessing liability. Although still relevant from a regulatory standpoint (particularly under FCC regulations) and under privacy laws (*see infra* § 50.06), whether Internet access is provided by a phone company or a cable or satellite provider does not impact a company's potential liability in litigation for third-party content based on its provision of Internet connectivity.

Today, the term *platform* is used to encompass a broad array of service providers who face particular liability risks for operating platforms used by third parties.

Similar risks are faced by website owners and app providers that allow user content on their sites or services. For websites and apps, the relevant distinctions to draw are based on interactivity. Sites with no interactive components face essentially no risk of liability for user content or misconduct on their sites or services. On the other hand, interactive locations where users may post, store or transmit material—whether ISPs, cloud service providers, social networks, blogs or corporate websites—face equivalent risks posed by User Generated Content (or user misconduct, which on the Internet manifests itself in the form of content), as do potentially sites that host these locations for third parties.

The terminology used to refer to different types of platforms and service providers has been complicated over the years by the fact that Congress has not used consistent definitions in the various statutes it has enacted relating to e-commerce. The Telecommunications Act of 1996, for example, governs conduct by users and providers of *Interactive Computer Services*, which is a term broadly defined to include virtually any networked computer (including corporate intranets), and treats interactive computer service providers the same as users in creating a broad exemption for indirect liability for a broad range of third-party content, including online acts of defamation. *See* 47 U.S.C.A. § 230; *see infra* § 49.04. The Digital Millennium Copyright Act, by contrast, governs conduct by *Service Providers*, which, like the term Interactive Computer Service, is broadly defined, but which by contrast may not apply to services owned by individuals or sole proprietorships. *See* 17 U.S.C.A. § 512;

may also be able to benefit by specific exemptions and immunities that can limit their exposure. Privity of contract al-

---

see infra § 49.05. The DMCA also distinguishes between *subscribers, account holders* and *users*, none of which are actually defined under the statute. Subscribers and account holders presumably have contractual or other relationships to service providers, which users need not have in order to access a site or service. *See supra* § 4.12.

The Protection of Children from Sexual Predators Act of 1998, which imposes reporting requirements on site owners and service providers in connection with child pornography posted, stored or transmitted online, uses the terms *Electronic Communication Service* and *Remote Computing Service*, which are given the same meaning as under the Electronic Communications Privacy Act of 1986. Specifically, an electronic communication service is defined as "any service which provides to users . . . the ability to send or receive wire or electronic communications." *See* 18 U.S.C.A. §§ 2258A(a)(1), 2510. A remote computing service, by contrast, refers to an entity that provides computer storage or processing services to the public by means of an electronic communications system. *See* 18 U.S.C.A. §§ 2258A(a)(2), 2711; *see generally infra* §§ 49.10[2] (reporting requirements), 50.06[4][D] (analyzing the distinctions between ECS and RCS providers).

Other statutes, including the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (the "CAN-SPAM Act"), 15 U.S.C.A. §§ 7701 to 7713, use the term *Internet Access Service*, which is defined to mean "a service that enables users to access content, information, electronic mail, or other services offered over the Internet, and may also include access to proprietary content, information, and other services as part of a package of services offered to consumers." 47 U.S.C.A. § 231(e)(4). The definition, however, excludes telecommunications services. 47 U.S.C.A. § 231(e)(4). As used under the CAN-SPAM Act, the term has been construed to include social networks. *See, e.g., MySpace, Inc. v. TheGlobe.com, Inc.,* Case No. CV 06-3391-RGK (JCx), 2007 WL 1686966 (C.D. Cal. Feb. 27, 2007); *see generally supra* § 29.03[7][C][ii]. The Ninth Circuit has held, however, that merely providing email accounts through third-party providers is insufficient to qualify a plaintiff as an Internet access service and has narrowly defined the term in cases where individuals or small companies with few users that outsource their services have sought standing to sue under the CAN-SPAM Act as Internet access services. *See Gordon v. Virtumundo, Inc.*, 575 F.3d 1040, 1051-52 (9th Cir. 2009); *see generally supra* § 29.03[7][C][ii] (analyzing standing and the definition of *Internet access service* in CAN-SPAM Act cases).

Ultimately, the lack of uniformity in either statutory or vernacular terminology reflects the dynamic nature of cyberspace and the difficulty of defining categories of providers in a medium where business models and technologies are constantly evolving. *See generally supra* § 1.06[9]. Congress presumably recognized this diversity (at least in some statutes) in choosing terms such as service provider, Internet access service and information location tools that are broadly defined and do not specifically correspondent to particular industry terms in use at the times they were enacted. *See infra* § 49.05.

lows platform providers to set rules governing use of the platform, to deter misconduct and to minimize the cost of disputes with their users through provisions such as binding arbitration. Service provider Terms and Conditions are analyzed in chapter 22. This chapter collects the specific liability risks, safe harbors and exemptions that platforms confront in dealing with third party rights owners and others typically not in privity of contract, as a result of user conduct or content or the operation of the platform itself. This chapter puts together in one place, in summary form, the third-party (or *secondary* or *vicarious*) liability risks and potential exemptions and immunities available to platforms. These issues are addressed in greater detail elsewhere in the treatise (as noted by cross-references in this chapter).

Any site or service that has any interactive component where users or other third-parties may post, store or transmit potentially infringing or illegal content face equivalent exposure for indirect liability for the conduct of their users.[2] The substantive standards for imposing third-party liability, however, are not uniform. Different risks and obligations may arise depending on the applicable substantive law. In addition, federal law provides certain safe harbors, exemptions and liability limitations to encourage particular practices, which potentially benefit some entities more than others. Individual businesses therefore should carefully evaluate their own potential exposure in operating online and in adopting policies and procedures (or drafting contracts and agreements, such as Terms of Use) to reduce their risk of loss.

Given the nature of the medium, *conduct* online manifests itself through *content*. Users interact via their mouse and

---

[2]Companies may face analogous third-party risks if they operate intranets or extranets and for employee use of social networks, microblogs such as Twitter and other Web 2.0 applications. *See generally infra* §§ 58.09 to 58.12 (intranets, extranets and use of social networking and microblogging tools). Web hosting companies also potentially may face liability risks for third-party conduct.

Passive website owners also potentially could be exposed to direct liability for the conduct of site operators, hosts, developers or other independent contractors for security breaches, service interruptions, linking or framing other websites or improperly using metatags to divert traffic to a site. *See generally supra* chapters 9 (links, frames, metatags, traffic diversion), 11 (ownership, employees and contractors), 19 (website development and hosting agreements), 27 (security); *infra* §§ 49.02 to 49.13 & chapters 50, 51 (cloud providers, hosts, storage lockers, social networks and blogs).

keyboard or mobile phone. User content, whether innocently posted or reflective of user misconduct, potentially exposes a site owner or service provider to liability. Sites that do not host third-party content and have no interactivity—which do not allow users to post, store or transmit material—face no liability for user misconduct (other than perhaps for hacking or other direct attacks on the site).[3]

As analyzed in section 49.02, there are certain unique attributes of cyberspace that create pressure to hold third-parties liable for online misdeeds. Interactive sites and services primarily face exposure from third-party acts of copyright infringement (which is analyzed in section 49.05 and potentially allows for large statutory damage awards that are disproportionate to any actual injury)[4] and to a lesser extent other forms of intellectual property infringement (which are addressed in sections 49.06 to 49.09), child pornography and obscenity (which are considered in section 49.10) and torts and other state law causes of action (and even some federal law claims) that may be preempted by the Telecommunications Act of 1996 (analyzed in section 49.04) or other illegal acts (section 49.13). Internet, mobile, cloud, social media and other e-Commerce businesses typically address these risks through policies and procedures. The limited risk of a site or service being held liable for false advertising for publicizing user generated content that turns out to be infringing is addressed in section 49.14.

The convergence of risks imposed on the conduct of e-commerce has resulted in a wide variation in practices. Rather than mandate particular conduct, Congress increasingly has opted to graft potential exemptions or safe harbors onto existing laws, which e-commerce businesses may elect to comply with or disregard without incurring additional liability. Whether a site owner or service provider chooses to benefit from these provisions should depend on: (1) the costs it would incur to satisfy statutory requirements; and (2) the liability risks associated with noncompliance. The importance of these factors will vary depending on a site's business model, its level of interactivity and the type of visitors

---

[3]Liability risks arising from a site's own conduct, including under privacy and security laws, and for compliance with federal statutes, such as the Americans with Disabilities Act, are analyzed in chapter 48. A compliance checklist is also included in that chapter.

[4]*See supra* § 4.14[2].

attracted to its site, among other things. The outcome of a cost/benefit assessment ultimately often depends on business and public relations considerations as much as the direct legal consequences associated with non-compliance.

This chapter addresses the particular legal risks posed by user conduct and content on interactive websites or services.[5] It provides a framework for evaluating third-party risks and outlines the different considerations which site owners and service providers should account for in crafting policies, practices and procedures to reduce their liability. It also analyzes the different models adopted by Congress to allow service providers and website owners to limit their liability for the most risky forms of conduct engaged in by third parties.[6] The remaining sections of this chapter outline the specific third-party liability risks faced by Internet sites and services that have any interactive features that allow users to post, store or transmit material. The chapter also briefly touches upon the liability exemptions created by the Cybersecurity Information Sharing Act (CISA).[7]

Building on the framework of this chapter, chapters 50 and 51 briefly outline additional unique risk factors faced by different types of Internet businesses, including cloud service providers and users (section 50.02), storage locker and file hosting services (section 50.03) and mobile providers (section 50.04). Issues involving social networks, blogs and other venues populated by user content are separately outlined in chapter 51. Chapter 51 also addresses special provisions on the protection of children in social networks. These chapters are intended to merely identify particular issues which are analyzed in greater depth elsewhere in the treatise (as noted by the cross-references found in the footnotes of each section).

Chapter 50 also analyzes the legal obligations of site owners and service providers to preserve the privacy of customer, subscriber and user contact information and communications and the circumstances under which this information may be disclosed. Among other things, user contact information is commonly sought by parties injured by anonymous or

---

[5] *See infra* §§ 49.04 *et seq*.

[6] *See infra* § 49.03.

[7] 6 U.S.C.A. §§ 1501 to 1510; *see generally supra* § 27.04[1.5].

pseudonymous tortfeasors and infringers,[8] whose ability to obtain redress from intermediaries increasingly has been circumscribed by legislative enactments and the adoption of more effective website and service provider policies and procedures (including contractual disclaimers and liability limitations).[9]

Chapter 48, the first chapter in this section of the treatise, provides a framework for evaluating direct liability risks, including a checklist for conducting a liability audit. Search engine liability is separately analyzed in chapter 9. Database protection, screen scraping and the use of bots is evaluated in chapter 5. Advertiser, marketing and promotions—including exposure for links, frames, metatags, keyword sales, banner advertisements, pop up ads and sponsored links—are analyzed in chapter 9.

Special issues governing liability and exemptions for domain name registrars and registries, and ways to mitigate liability, are analyzed in section 7.06.

Additional considerations for Network Service Providers (NSPs) are analyzed in section 4.12[14].

Terms of Use and provisions to reduce liability for sites and services are analyzed in chapter 22. Privacy Policies and liability are analyzed in section 26.14.

Special considerations for platforms and service providers in responding to subpoenas, warrants and court orders are addressed in section 50.06[4]. Section 50.06[4] also analyzes the Clarifying Lawful Overseas Use of Data Act (CLOUD Act), which is briefly discussed as well at the end of this chapter, in section 49.16.

49.02 Understanding Third-Party Liability in Cyberspace

Site owners and service providers, in addition to being held directly liable for their own acts and omissions, also face the risk of indirect liability for conduct that they may not know about or condone, and may be unable to prevent. While there may be sound policy reasons for holding third parties indirectly liable for conduct on *terra firma* that they could curb, with the proper incentive, these same considerations may not apply in cyberspace, where online providers

[8] *See infra* § 50.06.

[9] *See supra* chapters 21, 22 (online contracts and Terms of Use).

cannot as easily police the actions of third-parties. Ironically, the pressure for imposing indirect liability actually may be greater in cyberspace than on *terra firma*, even though the policy justifications for doing so may be weaker.

Cyberspace differs from the physical world in five principal respects that create pressure to hold third-parties—primarily site owners and service providers—indirectly liable for online misconduct.[1]

First, in cyberspace people may interact with relative anonymity. Anonymity and pseudonymity may embolden people to act in ways they would not on *terra firma*, and makes detection of the party primarily liable for online misdeeds or infringement more difficult.[2]

Second, in cyberspace all users interact on equal footing. Given the relatively low barriers to entry and costs of maintaining a presence online, the perpetrator of an Internet misdeed causing substantial injury may be a child, or an impoverished student or unemployed worker or other person unable to easily satisfy a large judgment.[3] Thus, to a greater extent than on *terra firma*, the person primarily liable for an

---

[Section 49.02]

[1]For a more complete discussion of legally significant differences between cyberspace and *terra firma*, *see supra* chapter 1; *see also* Ian C. Ballon, *Pinning the Blame in Cyberspace: Towards A Coherent Theory for Imposing Vicarious Copyright, Trademark and Tort Liability for Conduct Occurring Over the Internet*, 18 Hastings J. Comm. & Ent. L. 729, 733–35 (1996).

[2]For example, in *U.S. v. Baker*, 890 F. Supp. 1375 (E.D. Mich. 1995), *aff'd sub. nom United States v. Alkhabaz*, 104 F.3d 1492 (6th Cir. 1997), the defendant was charged under 18 U.S.C.A. § 875(c) with five counts of transmitting threats to injure or kidnap another in email messages transmitted over the Internet to "Gonda," an anonymous cyberfriend in Canada. To obtain a conviction in that case, the government would have had to show that the defendant's threats were real, and not merely idle—albeit perverse—chatter between college boys, which was difficult since the government was unable to identify the Canadian participant in the exchange of emails with the defendant. As an illustration of the potential difficulties associated with applying existing laws to cyberspace, the court wrote that " 'he' could be a 10-year-old girl, an 80-year-old man, or a committee in a retirement community playing the role of Gonda gathered around a computer." *United States v. Baker* also highlights that anonymity may be easier to maintain in international communications over the Internet. For further discussion of online anonymity, *see supra* § 1.06[1]. For an analysis of how to compel the disclosure of the identity of anonymous and pseudonymous tortfeasors and infringers, *see supra* § 37.02.

[3]Indeed, many of the more notorious acts of online misconduct early

online tort or infringement may not be a "deep pocket."

Third, because information is so easily available online, it is much easier for vigilant intellectual property owners and others to detect small scale fraud, misdeeds and infringement in cyberspace that, on *terra firma*, might go undetected. Thus, for example, many of the early reported Internet-related intellectual property infringement cases actually involved small time bulletin board operations[4] that in size and scale are probably no different from the record bootleggers of the 1970s or flea market vendors of unauthorized works. These outfits may be located more easily, however, because they are operating online, rather than in hundreds of discrete physical locations around the world. Similarly, defamatory words that on *terra firma* might be uttered in anger, in cyberspace are recorded without much more forethought on blogs or in email messages that can be saved, and copied, and more easily detected through simple search engine queries or via the Wayback Machine (www.InternetArchive.org).

Fourth, international boundaries dissolve over the Internet. Because cyberspace is an ethereal realm, online conduct actually may take place thousands of miles from where its effects are felt, creating potentially thorny jurisdictional problems and making it more difficult to locate or prosecute those directly responsible for Internet misdeeds.

Fifth, time moves much more rapidly in cyberspace, but in some respects eventually stands still. In fact, information moves so quickly that it may appear and disappear in a

---

on were perpetrated by college students. For example, *U.S. v. LaMacchia*, 871 F. Supp. 535 (D. Mass. 1994) involved an M.I.T. student; *U.S. v. Morris*, 928 F.2d 504 (2d Cir.), *cert. denied*, 502 U.S. 817 (1991), a Cornell graduate student; and *U.S. v. Baker*, 890 F. Supp. 1375 (E.D. Mich. 1995), *aff'd sub. nom United States v. Alkhabaz*, 104 F.3d 1492 (6th Cir. 1997), a University of Michigan student. The original Napster service (which was eventually shut down for copyright infringement, *see supra* § 4.11) likewise was created by a college student, Shawn Fanning, albeit one backed by venture capital investment.

[4]For example, *Playboy Enterprises, Inc. v. Frena*, 839 F. Supp. 1552 (M.D. Fla. 1993) involved a local BBS, where subscribers uploaded and downloaded bootlegged photographs, and *Sega Enterprises Ltd. v. MAPHIA*, 857 F. Supp. 679 (N.D. Cal. 1994) was brought against a BBS on which unauthorized copies of plaintiff's copyrighted videogames were uploaded and downloaded by subscribers.

moment's time.[5] Because information can appear and disappear rapidly in cyberspace, it is much more difficult for Internet providers to monitor conduct and content. The concept of Internet time, however, has not yet been fully incorporated into intellectual property infringement and fair use analysis.[6]

Online content ultimately can become immortal, making complete eradication of infringing or offensive material impossible.[7] A single individual may copy an entire website and repost it at a different location on the World Wide Web. Likewise, entire websites are archived and made available for posterity at InternetArchive.com.

The nature of online interaction creates strong incentives for plaintiff's counsel to hold access and content providers indirectly liable for acts and omissions occurring in cyberspace. Online infringers and tortfeasors may be more likely to be effectively "judgment proof" than their counterparts on *terra firma* because of low barriers to entry and because their conduct may have been undertaken anonymously, or they may be too young or poor to satisfy a damages award, or are located beyond the jurisdiction of a convenient and economical venue for litigation. As a consequence, and because the Internet has made detection of small scale fraud easier, a natural pressure exists to impose vicarious liability on more financially solvent defendants amenable to suit closer to home—namely site owners and service providers.[8]

At the same time, the policy justifications for doing so ap-

---

[5]For example, when a cybergraffiti artist defaced the U.S. Department of Justice website in August 1996, by the following day, all traces of the graffiti had vanished. Similarly, when President Obama took office in January 2009, at exactly Noon Eastern Standard Time the site located at WhiteHouse.Gov disappeared along with all traces of the Bush Administration and a completely new site appeared promoting the Obama Administration.

[6]*See supra* §§ 4.10[3], 10.11[4], and 11.04. For a more complete discussion of how cyberspace differs from *terra firma*, *see supra* chapter 1.

[7]It is not reasonable to hold Internet providers to the standard of insurers when a single person can create far greater damage online—and with significantly less effort—than would be required using traditional copying mechanisms on *terra firma*. Moreover, an online provider may be almost powerless to deter acts of infringement before they occur

[8]*See* Ian C. Ballon, *Pinning the Blame in Cyberspace: Towards a Coherent Theory for Imposing Vicarious Copyright, Trademark and Tort Liability for Conduct Occurring Over the Internet*, 18 Hastings J. Comm.

pear more attenuated. Cyberspace is not a physical location. Moreover, the manner and speed with which content, and indeed time itself, passes over the Internet make comparisons to *terra firma* incomplete. Traditional third-party liability doctrines developed in the physical world therefore should not be blindly applied online. For example, the doctrine of vicarious copyright liability—which holds that the owner of a physical location such as a flea market may be held liable for acts of infringement occurring on its property (regardless of its knowledge or intent) if it had: (1) the right and ability to control the conduct of the infringer; and (2) had a direct financial interest in the infringer's activities[9]—arose in part from the so-called "dance hall cases," in which owners of big band era dance halls were held liable when band leaders in their clubs played infringing songs, despite having been warned not to do so. In theory, a dance hall owner could run to the stage and prevent a wayward band leader from playing an infringing tune, much in the same way that the owner of a flea market arguably could patrol the grounds to ascertain whether blatantly infringing goods are being sold, and prevent infringing transactions from taking place.

It is not quite as easy to monitor the ethereal realm of cyberspace. A webmaster or service provider employee can only see what is before his or her eyes on a screen—not the invisible acts of copying that can occur in a digital environment. By the time infringing material is visible online, the act of infringement is likely complete. While goods lying on a flea market table are not themselves infringing, the mere act of posting information online creates a copy under the Copyright Act.[10] It therefore is not practical to expect that Internet providers can actually control conduct online. In fact, because information may be posted on a website or blog or transmitted by email in a matter of seconds, Internet providers cannot, as a practical matter, stop a determined infringer, or insure that infringing material is not widely disseminated. Congress's enactment of the DMCA, however, may have mooted these policy concerns by

---

& Ent. L. 729 (1996).

[9]*See supra* § 4.11; *infra* § 49.05[4].

[10]*See MAI Systems Corp. v. Peak Computer, Inc.*, 991 F.2d 511 (9th Cir. 1993), *cert. dismissed,* 510 U.S. 1033 (1994); *Religious Technology Center v. Netcom On-Line Communication Services, Inc.*, 907 F. Supp. 1361 (N.D. Cal. 1995); *see generally supra* § 4.04[3].

providing an easy mechanism for service providers to avoid liability.

49.03 Regulatory Models for Imposing Third-Party Liability in Cyberspace

The difficulties and potential unfairness associated with holding legitimate intermediaries such as site owners and service providers vicariously liable for online conduct that they generally cannot effectively control—as well as concern about the potentially retarding effect that the risk of such liability could have on the growth of e-commerce—led Congress to adopt a number of safe harbors and exemptions beginning with the Telecommunications Act of 1996, which was signed into law in January 1996. These laws, which include the Communications Decency Act, the Digital Millennium Copyright Act, the Child Online Protection Act, the Protection of Children from Sexual Predators Act of 1998, the Anticybersquatting Consumer Protection Act and the federal CAN-SPAM Act, generally have created incentives for Internet companies to engage in particular conduct in return for liability limitations, safe harbors or exemptions, rather than mandating particular conduct.[1]

Congress has not taken a uniform approach to limiting liability, even though site owners and service providers face a common problem—namely, the risk of exposure created by third-party users whose conduct cannot easily be controlled—under multiple state and federal civil and criminal laws that prohibit various different forms of content.[2] Certain regulatory trends have emerged, however, which may be relevant for companies to consider when evaluating how to structure their policies, practices and procedures.

Through the mid-1990s, Internet lawyers and businesspeople often differentiated between *content* and *access*

[Section 49.03]

[1]In contrast to most federal e-commerce laws, statutes governing adult content, including material that is obscene or which constitutes child pornography, generally compel or proscribe specific conduct, in addition to creating compliance incentives. *See infra* § 49.10.

[2]The lack of uniformity also is a function of the fact that the nature of e-commerce has changed significantly since the first Internet-related statute governing content, the Telecommunications Act of 1996, was signed into law.

providers.[3] Consistent with this demarcation, the criminal liability provisions of the ill-fated Communications Decency Act[4] (which largely were ruled unconstitutional on other grounds in *Reno v. ACLU*[5]) drew a number of distinctions between service providers, including content and access providers and employers, and offered a comprehensive model for assessing liability based on knowledge and intent.

Under the criminal provisions of the CDA, access providers were not subject to liability merely for providing a connection to the Internet.[6] Likewise, employers could not be held liable for acts of their employees or agents, unless such conduct was within the scope of employment, the employer had knowledge of the conduct, or authorized or ratified it, or the employer recklessly disregarded such conduct.[7] The Act also created safe harbors for providers that took reasonable measures in good faith to comply with the Act.[8] As explained in its legislative history, the defenses provided in the CDA were intended to "assure that attention is focused on bad actors and not those who lack knowledge of a violation or whose actions are equivalent to those of common carriers."[9]

Although it was a criminal statute, the CDA represented the first comprehensive liability scheme devised by Congress for assessing third-party liability in cyberspace. The CDA exempted access providers and employees from unintended liability and merely penalized knowing conduct, which placed the burden on aggrieved parties to affirmatively notify providers in order to assure a response (under the threat of subjecting them to liability for inaction in the face of notice or imputed knowledge). Yet, the statute recognized that even content providers could not be expected to act, in effect, as insurers of third-party conduct or content and therefore included safe harbors and defenses intended to encourage

---

[3] *See supra* § 41.01.

[4] 47 U.S.C.A. § 223.

[5] *Reno v. American Civil Liberties Union*, 521 U.S. 844 (1997); *see generally supra* § 41.02.

[6] 47 U.S.C.A. § 223(e)(1). In light of the U.S. Supreme Court's ruling in *Reno v. American Civil Liberties Union*, 521 U.S. 844 (1997), invalidating large portions of the CDA, the criminal provisions of the Act only apply to obscene communications.

[7] 47 U.S.C.A. § 223(e)(4).

[8] 47 U.S.C.A. §§ 223(e)(5), 223(f).

[9] Conference Report 104-458, 104th Cong. 2d Sess. 188 (1996).

interactive computer services to adopt measures to deter or prevent conduct proscribed by the Act, but not strictly penalize them if such measures were not entirely successful.[10]

The CDA model, premised on a provider's *knowledge* and *intent*, tracked the legal bases for imposing third-party liability in cases of contributory copyright infringement,[11] direct or contributory trademark infringement[12] and (prior to its enactment) online defamation;[13] although it arguably was more flexible in its implicit recognition of the limits to which third-party content could be controlled in cyberspace. The distinction drawn between *access* and *content*, in turn, was a logical corollary of the principle that liability should not be imposed absent knowledge or intent and was broadly consistent with the exemption that already existed under copyright law for passive carriers.[14]

Since the time the CDA was adopted, the lines between access and content have blurred and very few entities (other than backbone providers or commercial resellers that offer little more than connectivity) provide pure access without any content. Perhaps not surprisingly, subsequent statutes governing e-commerce generally have focused on particular conduct rather than attempting to distinguish among different types of internet service providers (which in any event

---

[10]These provisions were potentially more problematic in a criminal statute than they would have been in one imposing merely civil liability.

[11]*See infra* § 49.05[3]. Vicarious (and potentially even direct) copyright liability theoretically could be imposed on a service provider even absent knowledge or intent. *See infra* § 49.05[4].

[12]*See infra* § 49.06.

[13]*See supra* § 37.03. The analysis of a New York state court judge (in *Stratton Oakmont, Inc. v. Prodigy Services Co.*, Index No. 31063/94, 1995 WL 323710 (N.Y. Sup. May 26, 1995)) of what constituted imputed knowledge—and the related question of the limits of a service provider's ability to actually control third-party conduct or effectively monitor content online—ultimately led to the adoption of the Good Samaritan exemption codified at 47 U.S.C.A. § 230. *See supra* § 37.05. Congress also was cognizant of the well-publicized Netcom decision discussed in an earlier footnote in this subsection.

[14]*See* 17 U.S.C.A. § 111; *see infra* § 49.05[7]. The distinction between content and access also was recognized in Judge Ronald Whyte's analysis in his groundbreaking decision on third-party copyright liability, *Religious Technology Center v. Netcom On-Line Communication Services, Inc.*, 907 F. Supp. 1361 (N.D. Cal. 1995), which issued during the course of debate on what ultimately became the Telecommunications Act of 1996. *See generally supra* § 4.11 (analyzing the *Netcom* case).

has become increasingly difficult) or the level of service they offer.[15]

The first conduct-based statutory provision that did not distinguish among different types of providers was actually included in the CDA itself. The Good Samaritan exemption to the Telecommunications Act of 1996—which is a civil law provision incorporated in the Communications Decency Act—virtually eliminated republication and distributor liability for defamation in cyberspace (to overrule a 1995 court opinion which potentially could have had a chilling effect on the development of e-commerce press sites), as well as a host of non-IP state and federal claims premised on holding an intermediary liable as a publisher or speaker of third-party content, and created a broad exemption (in subpart 230(c)(2)(A)) from liability for conduct based on acts or omissions which otherwise could be inferred by an interactive computer service's[16] conduct in cyberspace.[17]

The Good Samaritan exemption was intended in large part to encourage networks and websites to screen and monitor their domains for adult content that could be viewed as inappropriate for children. While subpart 2 potentially provides broad immunity for "any action voluntarily taken in good

---

[15]An exception is the Child Online Protection Act (codified at 47 U.S.C.A. § 231) which, like the CDA, was a criminal statute, which focused on knowledge and intent. COPA regulated a specific form of content—sexual material directed to adults that may be deemed harmful to minors—and therefore included certain exemptions for entities which merely provided access to entities which themselves offered such content (among other service-based distinctions). *See* 47 U.S.C.A. § 231(b); *infra* § 49.10[4]. The exemptions created by COPA were only intended to apply to the extent that a provider engaged in exempted activity, however, out of recognition that providers often offer various different services including both access and content.

Congress also has enacted limited exemptions for providers that offer specific services. In particular, the Digital Millennium Copyright Act carves out a narrow exception for "Nonprofit Educational Institutions" that otherwise would be held liable for the acts of graduate student researchers and professors. *See supra* § 4.12[10]; *infra* § 49.05. The Anticybersquatting Consumer Protection Act similarly exempts domain name registrars and registries from third-party trademark liability under specific circumstances. *See supra* § 7.06[6]. These statutes, however, draw specific distinctions among providers, rather than more generally between access and content.

[16]The term interactive computer service is broadly defined. *See infra* § 49.04.

[17]*See supra* § 37.05; *infra* § 49.04.

faith to restrict access to or [the] availability of" particular content, it likely would not apply to a service provider or site owner that failed to undertake at least some *action* to further the objectives of the statute.[18] Similar exemptions were subsequently created for "*any action* taken in good faith to comply with" the mandatory reporting requirements of the Protection of Children from Sexual Predators Act of 1998[19] as well as for particular content deletions done "in a manner consistent with" the Good Samaritan exemption, pursuant to the Child Online Protection Act.[20]

The model created by the Good Samaritan exemption—of providing a legislative incentive to encourage particular conduct—was expanded in the Digital Millennium Copyright Act (DMCA) enacted by Congress and signed into law in late 1998. That statute created a broad exemption from liability for removing or disabling access to material believed to be infringing—to encourage service providers to police their domains and monitor content for the benefit of copyright owners. The DMCA also provides more narrow (but potentially more valuable) liability limitations to entities willing to adopt particular policies designed to discourage copyright infringement and, in the case of the user storage, linking and (in rare cases) system caching limitations, encourage adoption of notice and take down procedures for responding to complaints of copyright infringement.[21]

To avoid copyright liability for damages or attorneys' fees for infringing content stored at the direction of a user, a *service provider* (broadly defined to include both access and content providers), pursuant to the DMCA, must designate an agent with the U.S. Copyright Office (and list the agent's contact information on its website). DMCA agents receive statutory cease and desist communications called *notifica-*

---

[18]*See* 47 U.S.C.A. § 230(c)(2); *supra* § 37.05.

[19]42 U.S.C.A. § 13032(c) (emphasis added); *see generally infra* § 49.10[2].

[20]*See* 47 U.S.C.A. § 231(b)(4). COPA effectively expanded the scope of the Good Samaritan exemption created by section 230(c) to insulate from civil or criminal COPA liability under section 231, deletions of content "in a manner consistent" with section 230(c) which would not be considered to involve "selection or alteration of the communication" within the meaning of COPA. Congress presumably intended to encourage carriers and service providers to monitor and delete sexual content directed to minors. *See generally infra* § 49.10[4].

[21]*See generally infra* § 49.05.

tions (and in limited circumstances, formal replies termed *counter notifications*). In response to a notification, a service provider must take down—or literally remove or disable access to—allegedly infringing content.

The DMCA's notice and take down procedures implicitly recognize the limited ability of large service providers to actually know about or be able to evaluate the nature of content created by third parties, while also providing incentives for them to respond to complaints from copyright owners (and, at least in theory, disincentives to copyright owners or alleged infringers to file false notifications or counter notifications). These provisions, however, do not alter the underlying principles of copyright law which otherwise potentially allow for third-party liability to be imposed regardless of knowledge or intent.[22] Hence, where a defendant has chosen not to comply with the Act, or fails to meet its technical requirements, liability would be determined under existing case law. In litigation, no adverse inference may be drawn from a service provider's failure to comply.[23]

The DMCA is broadly consistent with the approach of the U.S. government in the 1990s to promote industry self-regulation.[24] It encourages (but does not compel) service providers to adopt "notice and take down" procedures and policies to discourage copyright infringement. The Anticybersquatting Consumer Protection Act similarly affords entities involved in registering domain names the opportunity to limit their liability by adopting specific policies.[25] The Good Samaritan exemption likewise is intended to promote (but not compel) content screening and monitoring.[26] Several statutes which were drafted to impose affirmative obliga-

---

[22]*See generally supra* § 4.11; *infra* § 49.05.

[23]*See supra* § 4.12.

[24]The government's role in re-shaping the Domain Name System in the late 1990s is perhaps the strongest expression of this policy preference. *See generally supra* § 7.02 (analyzing U.S. government position papers and chronicling the development of ICANN). The preference for industry self-regulation is also apparent in the provisions of the DMCA governing anti-circumvention devices, which contemplated the eventual adoption of industry standards known as standard technical measures. *See supra* § 4.21. The third-party liability limitations created by the DMCA, in turn, are only available to service providers that accommodate standard technical measures. *See supra* § 4.12[3].

[25]*See supra* § 7.06[6].

[26]Although Congress has shown a preference for creating incentives,

tions to control content, including the Child Online Protection Act of 1998 and the earlier-adopted Communications Decency Act, also included safe harbors or exemptions intended to encourage voluntary monitoring to promote safe environments and socially responsible conduct or, in the view of critics of these laws, censorship of free speech (which under the First Amendment likely could not be compelled). The Protection of Children from Sexual Predators Act of 1998 similarly exempts from other state or federal liability any action undertaken in good faith to promote compliance.[27]

In seeking to promote self-regulation, Congress by the late 1990s had moved away from the notion that knowledge of user misconduct could be inferred based simply on notice. The DMCA, for example, limits liability based on compliance with set procedures in response to a notification, but does not impose on service providers any obligation to evaluate the merits of a third-party claim (and indeed precludes them from doing so). Instead, Congress provided that liability could be imposed for signing false notifications or counter notifications.[28] Similarly, the Anticybersquatting Consumer Protection Act affords domain name registrars and registries certain exemptions for registering, transferring or refusing to register particular domain names in accordance with the terms of the statute, regardless of whether the domain name at issue eventually is found to infringe or dilute a mark.[29] Indeed, even the Good Samaritan exemption relieves an interactive computer service or user from having to evaluate the merits of a demand letter or other notice.

Although these statutes implicitly recognize that notice alone may not give a service provider enough information to evaluate the merits of an Internet-related dispute, they nonetheless are consistent with earlier views that liability for online conduct should only be based on knowledge or intent. While knowledge may not be inferred based on notice, notice may serve as a basis for a service provider undertaking par-

---

rather than mandating particular conduct, in particular cases (especially in connection with content, where First Amendment issues could arise), federal statutes governing e-commerce typically compel or proscribe particular conduct in addition to creating safe harbors, exemptions and liability limitations.

[27]*See infra* § 49.10[2].

[28]*See supra* § 4.12[9].

[29]*See* 15 U.S.C.A. § 1114(2)(D)(I)(I); *supra* § 7.06.

ticular actions which in turn would exempt it from liability. Moreover, intent continues to be relevant. The exemptions available under some statutes may not be available where a service provider acts intentionally, in bad faith or in the absence of good faith.[30]

Federal statutes that regulate third-party content or conduct in cyberspace have been grafted onto existing law, rather than fundamentally altering it.[31] The DMCA, for example, created liability limitations which service providers may choose to benefit from or simply ignore. Although potentially available to mitigate third-party liability for online conduct, these provisions do not otherwise change existing law. Other statutes governing direct liability for conduct occurring in cyberspace or otherwise regulating e-commerce similarly have been superimposed onto existing legal frameworks. For example, the Federal Trademark Dilution Act, which was passed by Congress in late 1995 in part to remedy cybersquatting (and which was subsequently

---

[30]For example, the Anticybersquatting Consumer Protection Act grants registries, registrars and others engaged in registration services a blanket exemption from damages under various provisions of the Lanham Act "for the registration or maintenance of a domain name for another absent a showing of bad faith intent to profit from such registration or maintenance of the domain name." *See* 15 U.S.C.A. § 1114(2)(D)(iii); *see generally supra* § 7.06. The Good Samaritan exemption likewise arguably does not apply when an interactive computer service provider or user acts with intent or actual knowledge (or knowledge imputed for reasons other than conduct undertaken on an interactive computer service). *See supra* § 37.05. The exemption available to adult content providers under the Child Online Protection Act, like the Good Samaritan exemption, presupposes a good faith undertaking aimed at compliance. *See infra* § 49.10[4]. A similar exemption is created by the Protection of Children from Sexual Predators Act of 1998 "on account of any action taken in good faith to comply" with its reporting requirements (including, presumably, content monitoring, although affirmative acts to monitor content are not required—at least in the absence of a complaint about or the discovery of material believed to constitute child pornography). *See* 42 U.S.C.A. §§ 13032(c), 13032(e); *see infra* § 49.10[2]. Likewise, the broad exemption for removing content available under the DMCA only applies where the content removed is believed in good faith to be infringing. *See* 17 U.S.C.A. § 512(g)(1); *supra* § 4.12[8].

[31]The Communications Decency Act and Child Online Protection Act—which are both criminal statutes directed expressly at sexual content—altered existing law and created safe harbors and broad exemptions intended to encourage particular conduct.

amended in 2006) does not preempt state remedies.[32] The Anticybersquatting Consumer Protection Act, passed four years later, similarly adds a new subsection to the Lanham Act (15 U.S.C.A. § 1125(d)) which plaintiffs may rely upon in addition to other remedies, but which otherwise does not change the standards for imposing liability for trademark infringement or dilution.

By creating both additional remedies to promote the development of e-commerce and civil law exemptions, safe harbors and optional liability limitations to encourage—but not compel—socially responsible acts, Congress has shaped the development of legal standards and industry self-regulation, but has left providers with a fair amount of discretion over whether and how to monitor or address complaints about third-party content. In response, businesses have adopted various different policies and procedures, depending on their corporate cultures and their assessments of their individual liability risks.

The approach to encouraging good practices in the development of e-commerce during its formative years in the 1990s was replicated more recently when Congress enacted the Cybersecurity Information Sharing Act (CISA),[33] which encourages, but does not require companies, to monitor their information systems, undertake defensive measures, and share cyber threat indicators and information about defensive measures, in the interest of promoting better security through greater cooperation.

As the Internet has matured, and businesses have expanded to the cloud, social media and mobile applications, the rules of the road have become both clearer and more complex. Any business that relies on user content, typically implements practices and procedures based on the protections of the Digital Millennium Copyright Act and the Good Samaritan exemption. Indeed, entire businesses have emerged as a result of the protection the DMCA and CDA provide to companies that otherwise might face crippling liability simply by operating online. While these laws provide clear demarcations, they are not always construed consistently with one another. For example, the Ninth Circuit has applied a broad "but for" test for evaluating entitlement to

---

[32] *See supra* § 6.11.

[33] 6 U.S.C.A. §§ 1501 to 1510; *supra* § 27.04[1.5] (analyzing the statute).

the DMCA safe harbor[34] for material stored at the direction of a user,[35] but rejected a similar test for CDA immunity under the Good Samaritan exemption.[36] The law governing Internet and mobile commerce also are subject to increasing volatility resulting from a turnover in the judiciary as federal court judges retire earlier to pursue lucrative mediation careers and are replaced by new appointees with less experience, hoping to make their mark by creating new law.

The following sections of this chapter outline in summary form the specific third-party liability risks faced by interactive Internet, mobile and cloud-based sites and services and the legal issues that businesses should evaluate in adopting practices and procedures to limit their liability for user misconduct and content. Each of the topics raised in this chapter are analyzed in substantially greater depth elsewhere in this treatise (as indicated within each of the following sections).

49.04 Non-IP Claims (Including Defamation and Other Torts)

Site owners and service providers may be able to avoid liability for User Generated Content in most civil suits, other than those for certain intellectual property violations,[1] by virtue of the Good Samaritan exemption created by the Telecommunications Act of 1996,[2] provided the material originated with a third party, and was not created by the

---

[34]If, but for the act of user storage, a service provider would not be exposed to liability for copyright infringement, then the service provider is entitled to the safe harbor (assuming it meets the other requirements for eligibility) regardless of what else it does with the material stored by the user on its site or service. *See UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1017 n.6 (9th Cir. 2013); *infra* § 49.05[1].

[35]17 U.S.C.A. § 512(c).

[36]Under the Good Samaritan exemption, 47 U.S.C.A. § 230(c)(1), the Ninth Circuit has expressly rejected application of a "but for" test to determine CDA immunity. *See Doe No. 14 v. Internet Brands, Inc.*, 824 F.3d 846, 853 (9th Cir. 2016) (explaining that "[p]ublishing activity is a but-for cause of just about everything Model Mayhem is involved in" and "the CDA does not provide a general immunity against all claims derived from third-party content."); *infra* § 49.04.

[Section 49.04]

[1]Intellectual property claims are separately addressed in this chapter. *See infra* §§ 49.05 (copyright), 49.06 (trademark), 49.07 (publicity), 49.08 (trade secret), 49.09 (patent).

[2]47 U.S.C.A. § 230(c).

site or service or its employees. The Good Samaritan exemption (also referred to as the Communications Decency Act, or CDA) was enacted to overrule a defamation case and protect children by encouraging sites and services to monitor and screen for adult material, but has been judicially construed far more broadly to reach virtually all third-party content, subject to narrow, enumerated exclusions, such as for certain IP claims.[3]

The Good Samaritan exemption inverted common law rules for imposing liability for defamatory acts occurring in cyberspace. On *terra firma*, distributors such as bookstores and news vendors enjoy a high level of First Amendment protection, and are liable for defamation only where they have actual or imputed knowledge. Republishers such as newspapers and magazines, however, may be subject to liability regardless of their knowledge or intent, since they exercise editorial control, and therefore—at least in theory—are better able to monitor content. Based on these well-established principles, site owners and service providers, prior to the enactment of the Telecommunications Act of 1996, sought to avoid screening material or exercising editorial control.[4] The Good Samaritan exemption, however, *encourages* monitoring and filtering of online content, and affords companies and individuals the opportunity to minimize their liability under the Act if they do the very things that on *terra firma* could subject them to liability as publishers.[5] As analyzed in greater detail in section 37.05, the Act broadly preempts inconsistent state laws[6] as well as providing immunity in response to certain federal claims based on

---

[3]*See supra* § 37.05[5].

[4]The applicability of this distinction in cyberspace was the subject of several significant decisions prior to the enactment of the Telecommunications Act of 1996. *See, e.g., Stratton Oakmont, Inc. v. Prodigy Services Co.,* Index No. 31063/94, 1995 WL 323710 (N.Y. Sup. May 26, 1995)); *Stern v. Delphi Internet Services Corp.*, 165 Misc. 2d 21, 626 N.Y.S.2d 694 (Sup. 1995); *Cubby, Inc. v. CompuServe, Inc.*, 776 F. Supp. 135 (S.D.N.Y. 1991); *see generally supra* §§ 37.03, 37.04.

[5]As analyzed in section 37.05, the term *publisher or speaker* has been broadly construed. It has even been held applicable to private Direct Messages. *See Fields v. Twitter, Inc.*, 217 F. Supp. 3d 1116, 1127-29 (N.D. Cal. 2016) (holding that Twitter acted as a publisher of Direct Messages sent by users, even though those messages are private and not available for public view, because the term *publisher* under the CDA should be broadly construed).

[6]*See* 47 U.S.C.A. § 230(e)(3). The Act does not prevent states from

content created by third parties where liability is premised on: (1) the site or service acting as a publisher or speaker of the material; or (2) any action taken in good faith to restrict access to or the availability of particular material.

Subpart (c)(1) provides that "[n]o provider or user of an interactive computer service[7] shall be treated as the publisher or speaker of any information provided by another information content provider."[8] This part of the exemption is self-executing and, by its terms, applies to any claim—not merely defamation—where liability is sought to be imposed on someone as the *publisher* or *speaker* of information provided by someone else. As discussed in section 37.05[1], this provision has been held to preempt state law claims for defamation, negligence, negligent misrepresentation, intentional infliction of emotional distress, harassment, tortious interference with contractual relations or business expectancy, breach of contract, privacy, waste of public funds, premises liability and nuisance (based on Internet use at a public library), and various state statutes, including consumer protection, unfair competition, Autographed Sports Memorabilia and anti-spamming laws.[9] Courts have also held that the CDA preempts claims based on conduct in the physical world, where the liability of a site or service is premised on its republication of third-party content, including claims brought by parents against Internet sites and services where children have met adults who then allegedly abused them.[10] In addition, the exemption has been applied to foreclose claims under the federal Computer Fraud and

---

enforcing laws consistent with the purpose of the "Good Samaritan" provision. 47 U.S.C.A. § 230(e)(3).

[7]An *interactive computer service* is defined under the Act 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 . . . ." 47 U.S.C.A. § 230(f)(2). An *access software provider* is defined as "a provider of software . . . or enabling tools that do any of the following: (A) filter, screen, allow or disallow content; (B) pick, choose, analyze, or digest content; or (C) transmit, receive, display, forward, cache, search, subset, organize, or translate content." 47 U.S.C.A. § 230(f)(4).

[8]An *information content provider* is defined as "any person or entity that is responsible, in whole or part, for the creation or development of information provided through the Internet or any other interactive computer service." 47 U.S.C.A. § 230(f)(3).

[9]*See supra* § 37.05[1][C] (citing cases).

[10]*See, e.g., Doe v. MySpace, Inc.*, 528 F.3d 413 (5th Cir.), *cert. denied,*

Abuse Act,[11] Fair Housing Act[12] and Civil Rights Act.[13]

Subpart (c)(2) goes beyond the issue of defamation liability and provides broad immunity from civil liability on account of—

(A) 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

(B) any action taken to enable or make available to information content providers or others the technical

---

555 U.S. 1031 (2008); *Doe v. MySpace, Inc.*, 629 F. Supp. 2d 663 (E.D. Tex. 2009); *Doe II v. MySpace Inc.*, 175 Cal. App. 4th 561, 96 Cal. Rptr. 3d 148 (2d Dist. 2009); *Doe v. America Online, Inc.*, 783 So. 2d 1010 (Fla. 2001); *see generally supra* § 37.05[3][B][ii] (analyzing the issue in greater detail and providing an exhaustive compendium of more recent case law treating conduct as content under the CDA). *But see Doe No. 14 v. Internet Brands, Inc.*, 824 F.3d 846 (9th Cir. 2016) (holding that the CDA did not bar a claim against the social networking site for models, Model Mayhem, based on the site's alleged failure to warn the plaintiff, a user of the site, of prior attacks on users by the two men who contacted her for an audition and then raped her, where the information that the site failed to warn about was obtained offline); *supra* § 37.05[3][B][ii] (analyzing *Doe No. 14*).

[11]*See Holomaxx Technologies Corp. v. Microsoft Corp.*, 783 F. Supp. 2d 1097 (N.D. Cal. 2011) (dismissing as preempted by section 230(c)(2) (with leave to amend) plaintiff's claim under the Computer Fraud and Abuse Act); *Holomaxx Technologies Corp. v. Yahoo!, Inc.*, No. CV-10-4926-JF, 2011 WL 865794 (N.D. Cal. Mar. 11, 2011) (ruling the same way in dismissing Holomaxx's virtually identical complaint against Yahoo!); *e360Insight, LLC v. Comcast Corp.*, 546 F. Supp. 2d 605 (N.D. Ill. 2008) (granting judgment on the pleadings in favor of Comcast under the section 230(c)(2) on claims for violations of the Computer Fraud and Abuse Act, 18 U.S.C.A. § 1030, infringement of free speech, tortious interference with prospective economic advantage and deceptive or unfair practices barred by the Illinois Consumer Fraud Act, arising out of Comcast's blocking email from e360, a bulk emailer, to Comcast subscribers).

[12]*See Chicago Lawyers' Committee for Civil Rights Under Law, Inc. v. Craigslist, Inc.*, 519 F.3d 666 (7th Cir. 2008) (holding the statute preempted by section 230(c)(1)). *But see Fair Housing Council v. Roommate.com, LLC*, 521 F.3d 1157 (9th Cir. 2008) (*en banc*) (remanding for further consideration plaintiff's Fair Housing Act claim and holding the defendant to be entitled to partial immunity under the CDA but also potentially liable as an information content provider for other aspects of its service); *see generally supra* § 37.05[3][C] (discussing both cases).

[13]*See Noah v. AOL Time Warner, Inc.*, 261 F. Supp. 2d 532 (E.D. Va. 2003); *see generally supra* § 37.05[2].

means to restrict access to material described in paragraph (1).[14]

Subpart (c)(2) is not self-executing. Sites and services should seek to maximize their potential protection under the Good Samaritan exemption by taking *any action* to restrict access to or the availability of the categories of content identified in section (c)(2)(A)[15] and to provide screening or filtering tools to benefit from the narrower exemption created by subpart (c)(2)(B). Action that could qualify a site owner or service provider for the exemption created by section (c)(2)(A) could include monitoring or screening for harassing or otherwise objectionable content. Whereas adopting or implementing a policy of reviewing or screening content could increase exposure on *terra firma*, doing so in cyberspace increases a site or service's potential protection. If a site monitors or screens for content, it cannot be held liable for anything undertaken in connection with monitoring or screening (such as the failure to find or properly identify particular material).[16] If a site takes no action, or does not do so in good faith, it will not be able to benefit from this exemption (although the exemption created by subpart (c)(1) may still apply).

Section 230(c) not only affords immunity for interactive computer service providers and users in U.S. litigation, but it also provides a defense to recognition or enforcement of a foreign judgment of defamation against an interactive computer service provider where liability would be inconsistent with section 230 had the judgment been entered in the United States.[17] The CDA itself has been construed to have some extraterritorial effect in that it applies to cases brought in the United States, regardless of where the claim arose or

---

[14]47 U.S.C.A. § 230(c)(2).

[15]Basic principles of statutory construction suggest that each of these terms usually should be construed to have independent meaning. *See generally supra* § 37.05[4].

[16]*See supra* § 37.05[4].

[17]*See* 18 U.S.C.A. § 4102(c); *supra* § 37.09[3] (analyzing the statute and its practical effects). This defense applies to interactive computer service providers only, not users, and only with respect to defamation which, while broadly defined, is still narrower than the full range of claims preempted by the CDA. *See supra* § 37.09[3] (analyzing the federal SPEECH Act).

what law applies.[18]

The California Supreme Court has held that a plaintiff cannot make an "end-run" on the CDA by obtaining a default judgment against an information content provider in a case where an interactive computer service provider could have asserted the CDA as a defense if it had been joined in the proceeding, and then seek to enforce an injunction obtained as part of the default judgment against the service provider, to have material taken down, without allowing the service provider to assert the CDA in the second action.[19]

The Good Samaritan exemption does not apply to "[f]ederal criminal statute[s,]"[20] "any law[s] pertaining to intellectual property,"[21] or the federal Electronic Communications Privacy Act[22] "or any similar State law."[23] The legislative history also makes clear that the exemption is not intended to

---

[18]*See Cohen v. Facebook Inc.*, 252 F. Supp. 3d 140, 158-60 (E.D.N.Y. 2017) (dismissing claims brought under Israeli law as preempted by the CDA because the conduct relevant to CDA analysis "must be where redress is sought and immunity is needed . . . ."); *see also Gonzalez v. Google, Inc.*, 282 F. Supp. 3d 1150, 1161-63 (N.D. Cal. 2017) (following *Cohen v. Facebook* in concluding that the CDA applied to claims brought by family members of a victim of the November 2015 ISIS terrorist attack in Paris, against Google, under the Anti-Terrorism Act, 18 U.S.C.A. § 2333(a), based on Google's ownership and operation of the YouTube platform, which plaintiffs alleged provided material support to terrorists, and dismissing those claims pursuant to the CDA).

[19]*See Hassell v. Bird*, 5 Cal. 5th 522, 234 Cal. Rptr. 3d 867 (2018); *see generally supra* § 37.05[8] (analyzing the case in greater detail).

[20]47 U.S.C.A. § 230(e)(1).

[21]47 U.S.C.A. § 230(e)(2); *see generally supra* § 37.05[5][B].

[22]47 U.S.C.A. § 230(e)(4). The Electronic Communications Privacy Act is comprised of two separate titles. The Wiretap Act, as amended by Title I of the Electronic Communications Privacy Act, 18 U.S.C.A. §§ 2510 to 2521, prohibits the unauthorized *interception* of electronic and aural communications, including email and other Internet communications. *See supra* § 44.06. Title II of the Electronic Communications Privacy Act, 18 U.S.C.A. §§ 2701 to 2711, also known as the Stored Communications Act, prohibits the intentional, unauthorized *access* of a facility through which an electronic communication is provided, to obtain, alter or prevent authorized access to a wire or electronic communication while stored electronically. *See supra* § 44.07. ECPA also governs a platform's response to subpoenas, warrants and court orders, which is separately addressed in section 50.06[4].

[23]47 U.S.C.A. § 230(e)(4).

limit potential liability for cancelbots.[24]

Pursuant to a 2018 amendment, certain provisions of the CDA also have no effect on particular claims involving sex trafficking: (A) any civil claim brought under 18 U.S.C.A. § 1595 (which authorizes private claims brought by victims under a number of statutory provisions), if the conduct underlying the claim constitutes a violation of 18 U.S.C.A. § 1591 (which penalizes sex trafficking of children, or by force, fraud, or coercion, or benefitting financially, including by advertising); (B) any state law criminal charge, if the conduct underlying a charge would constitute a violation of 18 U.S.C.A. § 1591 (which penalizes sex trafficking of children, or by force, fraud, or coercion, or benefitting financially, including by advertising); or (C) any state law criminal charge, if the conduct underlying a charge would constitute a violation of 18 U.S.C.A. § 2421A (which criminalizes promotion or facilitation of prostitution and reckless disregard of sex trafficking) if promotion or facilitation of prostitution is illegal in the jurisdiction where the defendant's promotion or facilitation of prostitution was targeted.[25] CDA immunity for federal criminal prosecutions under these statutes was already excluded by section 230(e)(1). The additional exclusions for state criminal proceedings and federal civil claims apply to CDA subsections 230(c)(1) (for republication of third party content)[26] and 230(c)(2)(B) (for enabling or making available content filters),[27] but not to the CDA defense created by subsection 230(c)(2)(A) (for voluntary, good faith action to restrict access to or the availability of certain adult content),[28] which may provide an exemption from liability for interactive computer service providers and users, if applicable.[29] The intent of the statute is to discourage interactive computer service providers and users from accepting adult service classified advertisements, similar to the ones that used to run on *Backpage.com*, and to encourage interactive computer service providers and users to avail themselves of the CDA exemption created by 230(c)(2)(A) for

---

[24]Conference Report 104-458, 104th Cong. 2d Sess. 194 (1996).

[25]47 U.S.C.A. § 230(e)(5); *see generally supra* § 37.05[5][C] (analyzing these provisions in greater detail).

[26]*See generally supra* § 37.05[3].

[27]*See generally supra* § 37.05[4].

[28]*See generally supra* § 37.05[4].

[29]*See* 47 U.S.C.A. § 230(e)(5).

good Samaritan actions to restrict access to adult content.[30] The scope of these various exclusions to the CDA are analyzed extensively in section 37.05. The 2018 amendments that address sex trafficking are analyzed in section 37.05[5][C]. The exclusion for laws pertaining to intellectual property, which is potentially relevant for most platforms, is analyzed in section 37.05[5][B].

As discussed in greater detail in section 37.05[5][B], there is presently disagreement over whether the CDA preempts state intellectual property laws (such as right of publicity, state trade secret and state trademark infringement claims, among others). The Good Samaritan exemption preempts any inconsistent state or local laws.[31] However, it may not be "construed to limit or expand any law pertaining to intellectual property."[32] In *Perfect 10, Inc. v. ccBill, Inc.*,[33] the Ninth Circuit construed the term "any law pertaining to intellectual property" to be restricted to "federal intellectual property"[34] and ruled that the plaintiff's right of publicity claim against an Internet payment processor was preempted.[35] The Ninth Circuit's analysis, however, has been criticized as inconsistent with the plain terms of the statute in two district court opinions from the First and Second

---

[30]*See supra* § 37.05[5][C] (analyzing the 2018 amendment and its purpose in greater detail).

[31]47 U.S.C.A. § 230(e)(3).

[32]47 U.S.C.A. § 230(e)(2).

[33]*Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102 (9th Cir.), *cert. denied,* 522 U.S. 1062 (2007).

[34]By Congressional action in 2016, a claim under the federal Defend Trade Secrets Act must be treated as a law that does not pertain to intellectual property, and therefore a DTSA claim may be precluded by the Good Samaritan exemption when brought against an interactive computer service provider or user. 18 U.S.C.A. §§ 1833 note, 1836 note, 1839 note; Pub L. 114-153 § 2(g), 130 Stat. 376, 382 (2016) ("This section and the amendments made by this section shall not be construed to be a law pertaining to intellectual property for purposes of any other Act of Congress."); *see generally supra* § 37.05[5][B] (analyzing the scope of CDA immunity in cases pertaining to intellectual property). The Good Samaritan exemption will not apply to claims brought under other federal IP statutes but, as noted in the text, may apply to state law IP claims, depending where suit is filed. This issue is analyzed extensively in chapter 37. *See supra* § 37.05[5][B].

[35]*Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102, 1118–19 (9th Cir.), *cert. denied,* 522 U.S. 1062 (2007).

Circuits.[36] While these district court opinions are not binding precedent in any circuit, given the sharp divergence between the Ninth Circuit's analysis, on the one hand, and more recent district court opinions challenging *ccBill* based on the plain text of the statute, on the other hand, courts in other parts of the country may be disinclined to find right of publicity claims necessarily preempted, at least at an early stage in the proceedings,[37] where the claim otherwise may be

---

[36]*See Atlantic Recording Corp. v. Project Playlist, Inc.*, 603 F. Supp. 2d 690 (S.D.N.Y. 2009) (construing the literal language of the statute as excluding claims pertaining to intellectual property and therefore allowing a common law copyright claim under New York law to proceed); *Doe v. Friendfinder Network, Inc.*, 540 F. Supp. 2d 288 (D.N.H. 2008) (holding that "any law pertaining to intellectual property" literally means any law—state or federal—and therefore denying the defendant's motion to dismiss plaintiff's right of publicity claim under New Hampshire law).

[37]*See, e.g., Doe No. 1 v. Backpage.com, LLC*, 817 F.3d 12, 26-27 & n.9 (1st Cir. 2016) (affirming dismissal of plaintiff's Massachusetts and Rhode Island right of publicity claims because there was no basis to infer that Backpage appropriated the commercial value of underage girls whose images were displayed in sex trafficking ads found on the site, where a publisher is merely a conduit and the party who actually benefitted from the misappropriation was the advertiser, but noting the split of authority over whether the CDA preempts right of publicity claims and plaintiff's argument that a right of publicity claim properly should not be thought of as an intellectual property claim); *Obado v.Magedson*, Civil No. 13-2382 (JAP), 2014 WL 3778261, at *7 & n.5 (D.N.J. July 31, 2014) (noting the Ninth Circuit's position but finding that the plaintiff failed to state a claim for a right of publicity violation and therefore it was unnecessary to decide whether the claim was excluded from CDA preemption), *aff'd on other grounds*, 612 F. App'x 90, 92 (3d Cir. 2015); *Amerigas Propane, L.P. v. Opinion Corp.,* Civil Action No. 12-713, 2012 WL 2327788, at *13 n.10 (E.D. Pa. June 19, 2012) (declining to consider whether plaintiff's claims arose from laws that pertain to intellectual property and were therefore excluded from CDA preemption because the court found that plaintiff adequately alleged that the claims arose from the defendant's own conduct to justify denying defendant's motion to dismiss); *Gauck v. Karamian*, 805 F. Supp. 2d 495, 499 n.3 (W.D. Tenn. 2011) (assuming, for purposes of plaintiff's motion for preliminary injunction, that plaintiff's Tennessee right of publicity claim fell within the CDA's statutory exclusion for claims that arise "from any law pertaining to intellectual property" but finding that a website's posting a reporter's name and likeness did not constitute a right of publicity violation); *Parisi v. Sinclair*, 774 F. Supp. 2d 310 (D.D.C. 2011) (declining "to extend the scope of the CDA immunity as far as the Ninth Circuit . . . ," but nonetheless dismissing plaintiff's right of publicity claim as barred by the newsworthiness exception); *Stayart v. Yahoo! Inc.*, 651 F. Supp. 2d 873 (E.D. Wis. 2009) (declining to exercise supplementary jurisdiction over state law claims and explaining in *dicta* the split of authority on the issue of whether a right of publicity claim

preempted by section 230(c).[38]

The split of authority also impacts copyright claims for sound recordings that pre-date 1972, which are not covered by the Copyright Act of 1976 and therefore may be asserted as common law claims. The interplay between common law copyrights, the CDA and the Digital Millennium Copyright Act is addressed in section 49.05[1].

The statute provides a potential exemption for both interactive computer service providers *and* users. The Act defines an *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 . . . ."[39] The exemption thus broadly reaches providers and users of both Internet sites and services and intranets, extranets and other computer networks, regardless of whether they are connected to the

---

based on third-party content is preempted by the CDA), *aff'd on other grounds,* 623 F.3d 436 (7th Cir. 2010); *see generally supra* § 37.05[5][B] (analyzing the issue in greater detail).

Stayart involved claims brought under Wisconsin law, which recognizes a common law tort for appropriation of a person's name or likeness and a statutory right based on "use, for advertising purposes or purposes of trade, of the name, portrait, or picture of any living person, without having first obtained the written consent of the person." 651 F. Supp. 2d at 887, *quoting* Wis. Stat. Ann. § 995.50(2)(b). Chief Judge Rudolph Rada noted that a right of publicity claim "is really an offshoot of the more general 'appropriation' tort, which compensates "bruised feelings" or other injuries to the "psyche," whereas the right of publicity "takes the next logical step" and gives individuals the "right of control over commercial use of one's identity . . . regardless of the infliction of emotional distress." 651 F. Supp. 2d at 887 *quoting* J. Thomas McCarthy, The Rights of Publicity and Privacy §§ 5.60, 5.67 (2d ed. 2008). Writing in *dicta*, Judge Rada explained that "the distinction between an appropriation theory and a right of publicity theory is . . . relevant to CDA immunity." 651 F. Supp. 2d at 887.

Even though Judge Rada previously had ruled that Yahoo! was entitled to CDA immunity, he wrote that a right of publicity claim "is generally considered an intellectual property claim, . . . which implicates that exception in § 230(e)(2)." 651 F. Supp. 2d at 887–88.

[38]In *Fraley v. Facebook, Inc.*, 830 F. Supp. 2d 785 (N.D. Cal. 2011), a district court in the Ninth Circuit ruled that plaintiffs' right of publicity claims against Facebook were not preempted where the court concluded that the basis for plaintiffs' claims was content that Facebook altered in ways that went beyond traditional (and privileged) editorial functions. *See supra* §§ 37.05[3][D][iii], 37.05[5][B] (analyzing the case).

[39]47 U.S.C.A. § 230(f)(2) (emphasis added).

Internet. As explained in the legislative history, the Good Samaritan "protections apply to all interactive computer services, as defined in new subsection 230 . . . , including non-subscriber systems such as those operated by many businesses for employee use."[40]

Based on the terms of the statute and case law the principal issue in most civil cases brought against Internet sites or services (except where one of the enumerated exclusions applies[41]) should[42] be whether the content at issue originated with a third party or whether the site or service itself could be deemed an *information content provider* and therefore potentially liable.

At least in the Ninth Circuit, in some cases a service provider could both be exempt from liability for certain content, while potentially at risk for other material. In the Ninth Circuit an interactive service provider also could be held liable as an information content provider to the extent user content was generated from mandatory questionnaires written by the provider itself.[43]

The Ninth Circuit clarified that CDA immunity in that circuit is not judged by a "but for" test.[44] In *Doe No. 14 v. Internet Brands, Inc.*,[45] the Ninth Circuit held that the CDA did not bar a claim by an aspiring model against the owners of Model Mayhem, a social networking site for people in the modeling industry, for negligently failing to warn her about two individuals who used the website as part of a scheme to lure her to a fake audition, where they proceeded to rape her, where the basis for the defendant's knowledge was in-

---

[40]Conference Report 104-458, 104th Cong. 2d Sess. 194 (1996).

[41]*See generally supra* § 37.05[5] (analyzing the exclusions in greater detail).

[42]The CDA may be raised as an affirmative defense, but some defendants do not do so in cases where it plainly should apply. The burden is on the defendant to raise an affirmative defense.

[43]*See Fair Housing Council v. Roommate.com, LLC*, 521 F.3d 1157 (9th Cir. 2008) (*en banc*) (remanding for further consideration plaintiff's Fair Housing Act claim and holding the defendant to be entitled to partial immunity under the CDA but also potentially liable as an information content provider for other aspects of its service); *see generally supra* § 37.05[3][C] (discussing the case and its implications).

[44]*Doe No. 14 v. Internet Brands, Inc.*, 824 F.3d 846, 853 (9th Cir. 2016); *see generally supra* § 37.05[3][B][ii] (analyzing the case and its implications).

[45]*Doe No. 14 v. Internet Brands, Inc.*, 824 F.3d 846 (9th Cir. 2016).

formation obtained offline. The court held that the plaintiff did not seek to hold Internet Brands liable as a publisher or speaker, but rather for its own failure to warn her about how third parties targeted and lured victims through Model Mayhem (which Internet Brands allegedly knew because it had sued the former owners of Model Mayhem in 2010 alleging that it faced liability for civil suits based the prior misconduct of the two men who went on to rape the plaintiff). As subsequently clarified in an amended opinion, the defendant's alleged knowledge, which formed the basis for plaintiff's duty to warn claim, "was obtained by Internet Brands from an outside source, not from monitoring postings on the Model Mayhem website."[46] The appellate panel conceded that Internet Brands acted as the "publisher or speaker" of user content by hosting the plaintiff's Model Mayhem profile and this action could have been described as the "but for" cause of her injuries because "[w]ithout it Flanders and Callum would not have identified her and been able to lure her to their trap" but the court wrote that "[p]ublishing activity is a but-for cause of just about everything Model Mayhem is involved in" and "the CDA does not provide a general immunity against all claims derived from third-party content."[47]

---

[46]*Doe No. 14 v. Internet Brands, Inc.*, 824 F.3d 846, 849 (9th Cir. 2016). *Doe No. 14* was decided in 2014, withdrawn in 2015 in response to a motion for reconsideration supported by amicus filings, and reissued in 2016 with edits to make clear that the duty to warn found not preempted in *Doe No. 14* arose from information learned offline. *See Doe No. 14 v. Internet Brands, Inc.*, 767 F.3d 894 (9th Cir. 2014), *reh'g granted, op. withdrawn*, 778 F.3d 1095 (9th Cir. 2015), *replaced by*, 824 F.3d 846 (9th Cir. 2016). As further clarified in the amended opinion, liability was not premised on Internet Brands learning of "predators' activity from any monitoring of postings on the website . . ." or from failing "to monitor postings at issue." *Doe No. 14 v. Internet Brands, Inc.*, 824 F.3d 846, 851 (9th Cir. 2016).

[47]*Doe No. 14 v. Internet Brands, Inc.*, 824 F.3d 846, 853 (9th Cir. 2016); *see generally supra* § 37.05[3][B][ii] (analyzing the case and its import in greater detail). By contrast, the Ninth Circuit has applied a "but for" test for evaluating when a service provider comes within the DMCA safe harbor for material stored at the direction of a user. If, but for the act of user storage, a service provider would not be exposed to liability for copyright infringement, then the service provider is entitled to the safe harbor (assuming it meets the other requirements for eligibility) regardless of what else it does with the material stored by the user on its site or service. *See UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1017 n.6 (9th Cir. 2013); *infra* § 49.05[1].

In *FTC v. Accusearch, Inc.*,[48] the Tenth Circuit arguably went even further than the Ninth Circuit in *Roommate.com* in broadly construing *information content provider,* thereby effectively narrowing the scope of the exemption potentially available to interactive computer service providers and users under section 230(c)(1). In *Accusearch*, the majority held that the defendant *developed* confidential telephone records originating with third parties merely by publishing them on its site and was *responsible* for this development because it solicited and then paid for them.

The Tenth Circuit's ruling in *Accusearch* departs from the approaches taken by other courts and suggests that site owners and service providers should be careful about the content they solicit and pay for, which could subject them to liability—at least in the Tenth Circuit.

The CDA is broadly applied in the First,[49] Second,[50] Third,[51]

---

[48]*F.T.C. v. Accusearch Inc.*, 570 F.3d 1187 (10th Cir. 2009).

[49]*See Small Justice LLC v. Xcentric Ventures LLC*, 873 F.3d 313, 321 (1st Cir. 2017) (affirming dismissal of claims for libel, intentional interference with prospective contractual relations, and certain aspects of plaintiff's unfair competition claim, brought against the operator of RipoffReport.com; rejecting arguments that the defendant should be liable as an information content provider for user comments because it (1) claimed copyright protection in its website content and (2) promoted content to be searchable on Google); *Doe No. 1 v. Backpage.com, LLC*, 817 F.3d 12, 18-24 (1st Cir. 2016) (affirming dismissal of claims for civil remedies under the Trafficking Victims Protection Reauthorization Act, 18 U.S.C.A. § 1595, and Massachusetts Anti-Human Trafficking and Victim Protection Act of 2010, Mass. Gen. Laws ch. 265, § 50, as preempted by 47 U.S.C.A. § 230(c)(1), in an opinion that was abrogated with respect to the federal trafficking claim, by the subsequent enactment of 47 U.S.C.A. § 230(e)(5)); *Universal Communication Systems, Inc. v. Lycos, Inc.*, 478 F.3d 413, 418 (1st Cir. 2007) (affirming dismissal of a claim brought by a publicly traded company against an Internet message board operator for allegedly false and defamatory postings by pseudonymous posters).

[50]*See Ricci v. Teamsters Union Local 456*, 781 F.3d 25, 26-28 (2d Cir. 2015) (holding that plaintiffs' claim for defamation against GoDaddy, as the website hosting service for the site where the allegedly actionable third party material was posted, was preempted by the CDA).

In *FTC v. LeadClick Media, LLC*, 838 F.3d 158 (2d Cir. 2016), the Second Circuit held that a defendant was not entitled to CDA immunity where it had participated in the development of the allegedly deceptive content at issue. The court also expressed skepticism that the operator of an affiliate marketing network could qualify as an interactive computer service provider where it routed customers, for a split second, through its HitPath server, before directing them to LeanSpa's website.

Fourth,[52] Fifth,[53] Sixth[54] and D.C.[55] Circuits. Subject to an arguably broader construction of the term *development* and,

---

[51]*See Obado v. Magedson*, 612 F. App'x 90, 91-94 (3d Cir. 2015) (affirming dismissal for failure to state claims for defamation, intentional and negligent infliction of emotional distress and invasion of privacy against various service providers, search engines and domain name registrars for republishing and allegedly manipulating search engine results to maximize the impact of allegedly defamatory content, based on the CDA); *Kabbaj v. Google Inc.*, 592 F. App'x 74 (3d Cir. 2015) (affirming dismissal of Kabbaj's claims against Google, Amazon, and Yahoo for defamation, tortious interference with contract, and negligent and intentional infliction of emotional distress under the CDA); *Green v. America Online (AOL)*, 318 F.3d 465 (3d Cir.) (holding AOL immune under the CDA from plaintiff's suit over allegedly defamatory material posted in its "Romance Over 30" chat room and for a computer virus sent to him from a third party), *cert. denied*, 540 U.S. 877 (2003).

[52]*See Westlake Legal Grp. v. Yelp, Inc.*, 599 F. App'x 481, 485 (4th Cir. 2015) (holding that a customer review site on which a third party allegedly posted defamatory remarks about the plaintiff was immunized by the CDA because operating an automated system that filters reviews is a traditional editorial function that did not render Yelp an information content provider); *Nemet Chevrolet, Ltd. v. Consumeraffairs.com, Inc.*, 591 F.3d 250 (4th Cir. 2009) (dismissing plaintiff's claim for defamation based on material posted by a third party); *Zeran v. America Online, Inc.*, 129 F.3d 327 (4th Cir. 1997) (holding a defamation claim based on a third party's posting on AOL preempted by section 230(c)(1)), *cert. denied*, 524 U.S. 937 (1998).

[53]*See Doe v. MySpace, Inc.*, 528 F.3d 413 (5th Cir.), *cert. denied*, 555 U.S. 1031 (2008).

[54]*See O'Kroley v. Fastcase, Inc.*, 831 F.3d 352 (6th Cir. 2016) (affirming dismissal of a suit brought against the Texas Office of Court Administration, Google, Fastcase and a German search engine by a man who falsely appeared to be listed as having been convicted of indecency with a child in search results because of the way the Texas Advance Sheet previewed information); *Jones v. Dirty World Entertainment Recordings LLC*, 755 F.3d 398 (6th Cir. 2014) (vacating and reversing a jury award for the plaintiff over highly offensive comments posted on a gossip website, based on the finding that defendants were entitled to immunity under the CDA).

[55]*See Bennett v. Google, LLC*, 882 F.3d 1163 (D.C. Cir. 2018) (applying *Klayman* and *Zeran* in holding that plaintiff's claims against Google for defamation, tortious interference with a business relationship, and intentional infliction of emotional distress, premised on Google's refusal to remove a user's blog post, in alleged violation of its "Blogger Content Policy," were preempted by section 2301(c)(1)); *Klayman v. Zuckerberg*, 753 F.3d 1354 (D.C. Cir. 2014) (affirming dismissal of negligence and intentional assault claims against Facebook and its founder because they did not create or provide the Facebook page that allegedly promoted religious hate and violence).

in the Ninth Circuit, several fact-specific exceptions, the CDA is also broadly construed in the Ninth,[56] and Tenth[57]

---

[56]*See, e.g.*, *Caraccioli v. Facebook, Inc.*, 700 F. App'x 588 (9th Cir. 2017) (affirming dismissal of plaintiff's claims for defamation, libel, false light, public disclosure of private facts, intrusion upon seclusion, intentional and negligent infliction of emotional distress, negligent supervision and retention, and California's Unfair Competition Law (UCL), "because the basis for each of these claims is Facebook's role as a 'republisher' of material posted by a third party, and the claims are, therefore, barred by the Communications Decency Act."); *Kimzey v. Yelp! Inc.*, 836 F.3d 1263 (9th Cir. 2016) (affirming dismissal of a defamation claim brought against Yelp over unfavorable customer reviews); *Riggs v. MySpace, Inc.*, 444 F. App'x 986 (9th Cir. July 25, 2011); *Barnes v. Yahoo!, Inc.*, 570 F.3d 1096 (9th Cir. 2009); *Fair Housing Council v. Roommate.com, LLC*, 521 F.3d 1157 (9th Cir. 2008) (*en banc*); *Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102 (9th Cir.), *cert. denied*, 522 U.S. 1062 (2007) (holding that the CDA preempted a right of publicity claim); *Batzel v. Smith*, 333 F.3d 1018, 1022, 1031, (9th Cir. 2003) (rejecting the argument that by minor wording changes and the addition of a "moderator's message" to a third-party posting (and by his decision to publish or not publish certain messages) a website owner was jointly responsible with the speaker as an information content provider); *Carafano v. Metrosplash.com. Inc.*, 339 F.3d 1119, 1120 (9th Cir. 2003) (holding an Internet dating site exempt under the CDA from liability for various claims arising out of a third party's submission of a phony profile purporting to belong to the plaintiff); *see also Zango, Inc. v. Kaspersky Lab, Inc.*, 568 F.3d 1169 (9th Cir. 2009) (broadly construing section 230(c)(2)(B)); *see generally supra* § 37.05[1] (analyzing Ninth Circuit law more extensively).

The Ninth Circuit has recognized certain fact-specific exceptions to CDA coverage. In *Barnes v. Yahoo!, Inc.*, 570 F.3d 1096 (9th Cir. 2009), the Ninth Circuit held that plaintiff's negligent undertaking claim was preempted by the CDA but ruled that her promissory estoppel claim was not, where the defendant allegedly affirmatively undertook to provide assistance in removing material that it would not otherwise have been required to remove under the CDA, but did not do so. Similarly, as discussed earlier in this subsection, in *Doe No. 14 v. Internet Brands, Inc.*, 824 F.3d 846 (9th Cir. 2016), the Ninth Circuit recognized an exclusion premised on a "duty to warn" arising from information obtained offline. *See generally supra* § 37.05[3][B][ii].

The Ninth Circuit also carved out a narrow exception in *Batzel v. Smith*, 333 F.3d 1018 (9th Cir. 2003), for communications that were not intended for further distribution, ruling that material "provided by another information content provider" necessarily means "provided" for publication, such that the exemption would not apply if the author never intended that a communication be posted. *Id.* at 1034.

[57]*See Silver v. Quora, Inc.*, 666 F. App'x 727 (10th Cir. 2016) (affirming dismissal of claims of libel and defamation brought by an investment banker against Quora, a question and answer website, over postings by two users, who allegedly used fake names in violation of Quora's Terms and Conditions to post allegedly defamatory statements about the

Circuits. The CDA has also been applied in the Seventh[58]

---

plaintiff); *Getachew v. Google, Inc.*, 491 F. App'x 923, 925-26 (10th Cir. 2012) (affirming dismissal of negligence and intentional infliction of emotional distress claims based on the results displayed by search engine queries and links to third party content about him because "Google cannot be held liable for search results that yield content created by a third party."); *Ben Ezra, Weinstein & Co., Inc. v. America Online Inc.*, 206 F.3d 980, 986 (10th Cir. 2000) (affirming summary judgment in favor of the defendant on plaintiff's claims for defamation and negligence based on the CDA). In *FTC v. Accusearch Inc.*, 570 F.3d 1187 (10th Cir. 2009), the Tenth Circuit purported to reaffirm the broad scope of *Ben Ezra*, *Weinstein & Co*. but held that an interactive service provider was liable as an information content provider where it solicited, paid for and sold the offending content at issue in the suit and suggested that such liability could be found whenever "it in some way specifically encourages development of what is offensive about the content." *Id.* at 1199. As discussed in section 37.05, *Accusearch* may be best explained in terms of its unique facts.

[58]*See Chicago Lawyers' Committee for Civil Rights Under Law, Inc. v. Craigslist, Inc.*, 519 F.3d 666, 668–69 (7th Cir. 2008) (holding a claim under the Fair Housing Act preempted by section 230(c)(1)); *see also Doe v. GTE Corp.*, 347 F.3d 655 (7th Cir. 2003) (affirming dismissal of a claim by college athletes who were secretly video-recorded in locker rooms, bathrooms and showers, against the companies that provided Internet access and web hosting services to sites that sold copies of these videos; discussing the CDA extensively in *dicta*).

Former Chief Judge Easterbrook, who wrote the opinions in both *Craigslist* and *GTE Corp.*, subsequently cited both cases in *Chicago v. StubHub, Inc.*, 624 F.3d 363, 366 (7th Cir. 2010) for the proposition that "subsection (c)(1) does not create an 'immunity' of any kind." In *Chicago v. StubHub*, the Seventh Circuit held that a suit by the City of Chicago asserting that an Internet ticket resale service was responsible for collecting a special city amusement tax on ticket sales was not preempted by the CDA. Judge Easterbrook wrote that subsection (c)(1) "limits who may be called the publisher of information that appears online. That might matter for defamation, obscenity, or copyright infringement. But Chicago's amusement tax does not depend on who 'publishes' any information or is a 'speaker.' " *Id.*; *see also Lansing v. Southwest Airlines Co.*, 980 N.E.2d 630 (Ill. App.) (applying Seventh Circuit law in ruling that plaintiff's negligent supervision claim was not preempted by the CDA because section 230(c)(1) "limits who may be called the publisher or speaker of information that appears online . . . [and therefore] could foreclose any liability that depends on deeming the ICS user or provider a publisher or speaker . . . [but] was not enacted to be a complete shield for ICS users or providers against any and all state law torts that involve use of the Internet."), *appeal denied*, 979 N.E. 2d 878 (Ill. 2012).

In *Huon v. Denton*, 841 F.3d 733 (7th Cir. 2016), the appellate court reversed and remanded the lower court's order dismissing defamation and false light claims asserted by an accused rapist against Gawker over user comments posted on Gawker's website in connection with an article Gawker had published about plaintiff Huon suing the website Above the

and Eighth[59] Circuits.

Courts have held that platform providers do not *develop* content, and therefore may not be held liable as information content providers, for providing social media tools, such as access to Twitter and YouTube, because the provision of neutral tools, including targeted advertising, does not equate to content development.[60]

More recent case law (as well as circuit-by-circuit and claim-by claim analysis of CDA opinions) is set forth in section 37.05.

If a site owner or service provider is not exempt from liability under subpart (c)(1), the next question should be whether the exemption created by subpart (c)(2)(A)[61] is available because liability is premised on any action, undertaken

---

Law for implying that he was a rapist in an article published on the same day he was acquitted of rape, entitled "Acquitted Rapist Sues Blog for Calling Him Serial Rapist." Judge Williams, writing for himself, Judge Easterbrook and Southern District of Illinois Judge Yandle (who was sitting by designation), explained that although the "Gawker Defendants may well be correct in contending that none of Huon's various allegations actually occurred, . . ." they had stated a claim by alleging that some of the allegedly defamatory comments had been authored by Gawker employees, allegedly to generate revenue. *Id.* at 741-43. Judge Williams wrote that "[d]iscovery is the proper tool for Huon to use to test the validity of his allegations, and if he is unable to marshal enough facts to support his claim the Gawker Defendants can move for summary judgment." *Id.* at 742. The court declined to parse through Huon's specific allegations, most of which Gawker alleged amounted to traditional publishing activities insulated by the CDA, because it did not need to "wade into that debate, since at least some of the allegedly defamatory comments were authored by Gawker employees—thus making Gawker an 'information content provider' under § 230(f)." *Id.* at 743.

[59]*See Johnson v. Arden*, 614 F.3d 785, 791-92 (8th Cir. 2010) (holding that plaintiffs' defamation claim against an ISP that provided hosting services to www.ComplaintsBoard.com, where allegedly defamatory statements about plaintiffs' Kozy Kittens Cattery business had been posted, was preempted by the CDA because sections 230(c)(1) and 230(e)(3) collectively "bar[red] plaintiffs from holding ISPs legally responsible for information that third parties created and developed" and the record contained no evidence that the InMotion, the ISP, "designed its website to be a portal for defamatory material or do anything to induce defamatory postings.").

[60]*See Pennie v. Twitter, Inc.*, 281 F. Supp. 3d 874, 890-92 (N.D. Cal. 2017); *Gonzalez v. Google, Inc.*, 282 F. Supp. 3d 1150, 1168-69 (N.D. Cal. 2017); *see generally supra* § 37.05[3][D].

[61]Section (c)(2)(B) creates an exemption for a narrower circumstance where liability is premised on any action taken to enable or make avail-

in good faith, to restrict access to or the availability of material that is adult in nature or harassing or otherwise objectionable.[62]

If the Good Samaritan exemption does not apply, a site or service's exposure for defamation or other speech-based torts will depend, in part, on whether it is treated as a publisher or distributor under the pre-CDA case law discussed above and the standards generally applicable in the physical world.[63] This issue is addressed in greater detail in section 37.05[10]. The standards for liability for other causes of action potentially preempted by the CDA, such as Civil Rights or Fair Housing Act claims, would be determined by their terms.

International issues and U.S. restrictions imposed on the enforcement of certain defamation judgments obtained in other countries under the SPEECH Act are analyzed in section 37.09.

49.05 Copyright Liability

49.05[1] Third-Party Copyright Liability—In General

Site owners and service providers may face significant exposure for copyright liability for User Generated Content unless they comply with the liability limitation provisions of the Digital Millennium Copyright Act (DMCA).[1] The DMCA potentially provides a complete defense to liability for dam-

---

able to information content providers or others the technical means to restrict access to material described in paragraph (1).

[62]As noted earlier in this section, the provision creates an exemption when liability is premised on any action taken in good faith to restrict access to or the 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.

[63]*See supra* § 37.04.

[Section 49.05[1]]

[1]*See* 17 U.S.C.A. § 512(c); *Viacom Int'l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 38–40 (2d Cir. 2012) (holding that transcoding and displaying user videos, among other things, were insulated from liability by the DMCA's user storage safe harbor); *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1015-20 (9th Cir. 2013) (affirming summary judgment for a user submitted video site, holding that transcoding, streaming and allowing downloading of user videos did not undermine safe harbor protection); *Io Group, Inc. v. Veoh Networks, Inc.*, 586 F. Supp.

ages or attorneys' fees for federal (and state common law or statutory[2]) copyright infringement claims based on material stored at the direction of users (such as User Generated Content) and links or other information location tools that lead to infringing material.[3] The scope of potential protection is very broad. The Second and Ninth Circuits apply a "but for" standard of general causation, rather than a proximate cause test, in evaluating whether a claim is based on material stored at the direction of a user, and therefore subject to

---

2d 1132 (N.D. Cal. 2008) (granting summary judgment for Veoh, holding it was entitled to the DMCA safe harbor); *infra* § 49.05[2]; *supra* § 4.12.

[2]Although the Copyright Act broadly preempts state law claims "that are equivalent to any of the exclusive rights within the general scope of the Copyright Act" (17 U.S.C.A. § 301; *supra* § 4.18[1]), sound recordings fixed prior to February 15, 1972 are not entitled to federal copyright protection and therefore may be the subject of suits brought for infringement of common law and state statutory copyrights (which otherwise generally are preempted by the federal Copyright Act). *See, e.g., Capitol Records, Inc. v. Naxos of America, Inc.*, 4 N.Y.3d 540, 797 N.Y.S.2d 352, 830 N.E.2d 250, 263–64 (2005); *Arista Records LLC v. Lime Group LLC*, 784 F. Supp. 2d 398, 437 (S.D.N.Y. 2011); *see generally supra* § 4.18[2] (analyzing state common law and statutory copyright law protection for sound recordings fixed prior to February 15, 1972).

The Second Circuit has held that the Digital Millennium Copyright Act, 17 U.S.C.A. § 512, provides safe harbor protection for service providers for claims of state law copyright infringement of sound recordings fixed prior to February 15, 1972, in addition to claims brought under federal law. *See Capitol Records, LLC v. Vimeo, LLC*, 826 F.3d 78, 87-93 (2d Cir. 2016); *see generally supra* § 4.12[19].

A claim against an intermediary for state law copyright infringement based on user content and conduct would be preempted by the Communications Decency Act, 47 U.S.C.A. § 230(c), in the Ninth Circuit but not necessarily in New York or some other jurisdictions. *Compare Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102 (9th Cir.) (construing the term "any law pertaining to intellectual property" to be restricted to "federal intellectual property" and therefore holding that the plaintiff's right of publicity claim against an Internet payment processor was preempted), *cert. denied,* 522 U.S. 1062 (2007) *with UMG Recordings, Inc. v. Escape Media Group, Inc.*, 948 N.Y.S. 881, 888-89 (N.Y. Sup. 2012), *rev'd on other grounds,* 107 A.D.3d 51, 964 N.Y.S.2d 106 (N.Y. App. 2013); *Doe v. Friendfinder Network, Inc.*, 540 F. Supp. 2d 288 (D.N.H. 2008) (holding that "any law pertaining to intellectual property" literally means any law—state or federal—and therefore denying the defendant's motion to dismiss plaintiff's right of publicity claim under New Hampshire law) *and Atlantic Recording Corp. v. Project Playlist, Inc.*, 603 F. Supp. 2d 690 (S.D.N.Y. 2009) (construing the literal language of the statute the same way as the court in *Doe* and allowing a common law copyright claim under New York law to proceed); *see generally supra* §§ 49.04, 37.05[5][B].

[3]*See* 17 U.S.C.A. § 512(d); *infra* § 49.05[2]; *supra* § 4.12.

the safe harbor.[4] If, but for the act of user storage, a service provider would not be exposed to liability for copyright infringement, then the service provider is entitled to the safe harbor (assuming it meets the other requirements for eligibility) regardless of what else it does with the material stored by the user on its site or service.[5] To benefit from the safe harbor, however, a service provider must meet a number of specific, technical requirements (as described below briefly and analyzed more extensively in section 4.12). The statute compels site owners and service providers to do more than merely honor the DMCA's notice and takedown procedures to benefit from its safe harbors. If a site removes 100% of the items identified in DMCA notices, but fails to comply with the other technical provisions of the statute, it will not be entitled to the DMCA's safe harbors.

All interactive sites and services potentially risk liability for copyright infringement based on the acts of their users. While the risk of exposure for merely creating a link to infringing content is small for any legitimate service that did not create the link specifically to encourage infringement (and which disables links to infringing sites when given notice),[6] the risk of unintended liability based on user storage potentially is significant and cannot easily be prevented. Where liability may be established, damages potentially can be significant (and are determined by a judge or jury, subject

---

[4]This analogy was articulated expressly by the Ninth Circuit. *See UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1017 n.6 (9th Cir. 2013). It is also consistent with the way the Second Circuit construed the DMCA's user storage safe harbor in *Viacom Int'l, Inc. v. YouTube, Inc.*, 676 F.3d 19 (2d Cir. 2012); *see also BWP Media USA, Inc. v. Clarity Digital Group, LLC*, 820 F.3d 1175, 1180-82 (10th Cir. 2016) (broadly defining *user* for purposes of storage "at the direction of a user," in affirming summary judgment for the operator of Examiner.com based on its entitlement to the DMCA safe harbor).

[5]By comparison, under the Good Samaritan exemption, 47 U.S.C.A. § 230(c)(1), the Ninth Circuit has expressly rejected application of a "but for" test to determine CDA immunity. *See Doe No. 14 v. Internet Brands, Inc.*, 824 F.3d 846, 853 (9th Cir. 2016) (explaining that "[p]ublishing activity is a but-for cause of just about everything Model Mayhem is involved in" and "the CDA does not provide a general immunity against all claims derived from third-party content."; *see generally supra* §§ 49.04 (CDA immunity generally), 37.05[3][B][ii] (analyzing the case and its import in greater detail).

[6]*See supra* §§ 9.02 to 9.04 (analyzing liability for links), 4.12[1] (discussing liability in the context of the DMCA), 4.12[7] (outlining the liability limitation).

to a deferential standard of review on appeal). Where a copyright owner has registered its copyrights prior to the time they were infringed, it may recover statutory damages of between $750 to $30,000 *per work infringed* (i.e., per television episode, photograph, video or computer program),[7] increased to $150,000 per work infringed where a plaintiff can prove that the infringement was willful (or reduced to as low as $200 per work infringed if a defendant can prove that its infringement was innocent).[8] Thus, where a lot of works are at issue, the range of potential exposure could be large (and if the copyright owner timely registered its work, it may also recover its attorneys' fees).[9] Conversely, a copyright owner may elect to recover its actual damages *and*, to the extent not duplicative, a defendant's profits.[10] Thus, where the copyright owner incurred significant losses and/or the defendant profited substantially, damages also could be large.

Any site or service that hosts interactive areas where users may post, store or transmit material risks liability for user content or conduct because of the ease with which material such as text, photos, music, software, graphics and video may be copied. Simply posting or transmitting protected works online may simultaneously constitute acts of reproduction or distribution and potentially also amount to public performances or displays under the Copyright Act.[11] An act of infringement therefore may be complete at the very moment material is posted or transmitted (or in the case of a reproduction, stored, played or viewed on a computer screen) without authorization. Copyright liability also generally may be imposed without a showing of either knowledge or intent[12] (although as a practical matter most sophisticated copyright owners prefer to send notifications to afford sites and services an opportunity to remove infringing material or risk exposure for contributory liability by failing to act in the face of notice).

When complaints are lodged, it is equally difficult for site

---

[7] *See supra* § 4.14[2][B] (analyzing what constitutes a *work*).

[8] *See* 17 U.S.C.A. § 504; *supra* § 4.14[2].

[9] *See supra* § 4.15.

[10] *See supra* §§ 4.14[1] (election between actual and statutory damages), 4.14[3] (actual damages and profits), 4.14[4] (alternative theories of recovery in Internet cases).

[11] *See supra* §§ 4.03, 4.04[3].

[12] *See supra* § 4.11.

owners and service providers to evaluate the merits of a claim. Copyrighted material need not contain a copyright notice to enjoy protection under U.S. law, making it often difficult or impossible to evaluate whether a given work is protected. It is also extremely difficult for a site or service to evaluate whether a given user submission is licensed, a fair use or otherwise permitted. If a site complies with the DMCA, it need not make these difficult evaluations. It simply disables access to or removes material or links identified in substantially complying DMCA notifications. Users who believe that their material was removed in error because they have a lawful right to it, may seek to have it restored by submitting a counter notification (although service providers need not comply with counter notifications to limit their liability for infringement). The DMCA effectively shifts the burden to copyright owners and users to resolve disputes directly through litigation, rather than forcing a site owner or service provider, as the intermediary, to determine whether a particular piece of content is protected, infringing, licensed or permitted as a fair use. Absent the DMCA safe harbors, site owners and service providers must try to make these determinations when complaints are lodged, or risk liability for contributory infringement.[13]

To ensure the integrity of the system, the DMCA authorizes damages and potentially attorneys' fees on copyright owners and users who make misrepresentations in DMCA notifications or counter notifications[14] and, by judicial extension, on copyright owners that fail to consider fair use before sending a DMCA takedown notice.[15]

The current copyright statute was enacted in 1976 and incorporates secondary (or "third-party") liability principles developed under the preceding 1909 Act. Third-party liability for copyright infringement may be imposed under theories of direct, contributory and vicarious liability. Pursuant to the

---

[13]*See supra* § 4.11[3].

[14]*See* 17 U.S.C.A. § 512(f); *supra* §§ 4.12[9][D], 4.12[9][F].

[15]*See Lenz v. Universal Music Corp.*, 815 F.3d 1145 (9th Cir. 2016) (holding that a copyright owner must have a subjective good faith belief that allegedly infringing material does not constitute a fair use before sending a DMCA takedown notice and that failing to form such a subjective good faith belief, or being willfully blind, would justify the imposition of sanctions under 17 U.S.C.A. § 512(f)); *see generally supra* §§ 4.12[9][D], 4.12[9][F] (discussing the case at greater length), 4.10[1] (analyzing fair use).

U.S. Supreme Court's decision in *MGM Studios, Inc. v. Grokster, Ltd.*,[16] liability also may be imposed for inducing copyright infringement,[17] under standards that are somewhat analogous to patent or trademark inducement,[18] where an intent to induce user infringement is shown. In most cases involving legitimate site owners or service providers who have no intention of encouraging infringement, inducement will not apply (although it may be pled in a suit against a service provider because it places at issue a defendant's intent and therefore potentially opens up much broader discovery than otherwise might be permitted). Where liability has been imposed on sites or services for user material or misconduct, it has generally been premised on contributory or vicarious liability (although direct liability also may be imposed where the site or service engaged in direct action or volitional conduct to further acts of infringement). The fair use defense and, in rare instances, *de minimis* copying, may insulate a site or service from liability. As a practical matter, however, suits against sites and services for user content may be very fact-specific and therefore potentially expensive to defend if a site does not qualify for the DMCA safe harbor.

Although the DMCA provides an affirmative defense to a claim of infringement, often the best starting point for limiting (or evaluating potential) service provider liability is with the DMCA, rather than the specific grounds on which liability may be imposed. If the DMCA applies, a site owner or service provider may not be held liable for damages or attorneys' fees for infringement resulting from material stored at the direction of a user or for links or other information location tools. If it is inapplicable, then parties must evaluate whether liability may be imposed for direct, contributory, vicarious or inducing copyright infringement and whether other defenses, such as fair use, may apply.

The following subsections provide a brief overview of the DMCA and the major liability theories and defenses that may arise in a suit over user content or misconduct. These issues are analyzed in substantially greater depth in chapter

---

[16] *Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd.*, 545 U.S. 913 (2005).

[17] *See infra* § 49.05[3][E].

[18] *See infra* §§ 49.06 (trademark inducement as grounds for contributory infringement), 49.09 (patent inducement).

4 in sections 4.12 (the DMCA safe harbors), 4.11 (secondary liability for user content) and 4.10 (fair use).

49.05[2] The DMCA Safe Harbors

The Digital Millennium Copyright Act (DMCA)[1] provides four liability limitations and one broad exemption for *service providers* that would like to take advantage of them and are willing to meet the specific requirements of the Act. The DMCA also creates a special liability limitation for Nonprofit Educational Institutions (NEIs), but otherwise does not distinguish between different kinds of service providers.[2] The DMCA is simply grafted onto existing law and does not alter the standards for indirect liability. Thus, a company's failure to comply with the DMCA or meet its technical requirements may not be cited as evidence of liability.[3]

The DMCA provides liability limitations,[4] or safe harbors,

[Section 49.05[2]]

[1]17 U.S.C.A. § 512. The DMCA is exhaustively analyzed in section 4.12. The brief summary set forth in this chapter on liability for user content and misconduct is intended to provide an overview of liability, rather than supplant the full analysis set forth in section 4.12.

[2]*See supra* § 4.12[10]. The NEI liability limitation will not apply to commercial services that host user generated content and therefore is not separately discussed in this chapter. It is analyzed extensively in chapter 4.

[3]*See supra* § 4.12.

[4]The DMCA liability limitations insulate a service provider from liability for damages or attorneys' fees, but are not exemptions from liability (meaning that others may be held liable for the same infringing acts). The DMCA also provides that service providers may be subject to narrow injunctions in particular circumstances, although copyright owners rarely take advantage of this provision and service providers usually cooperate with copyright owners such that injunctive relief is not necessary. *See supra* § 4.12.

At least in the Ninth Circuit, an injunction compelling a service provider to remove user content is deemed to be a mandatory injunction, which is disfavored. *Garcia v. Google, Inc.*, 786 F.3d 733, 740 & n.4 (9th Cir. 2015) (*en banc*); *see generally supra* § 4.13[1] (setting forth the standards for obtaining injunctive relief). It may also be viewed as an impermissible prior restraint. *See Garcia v. Google, Inc.*, 786 F.3d 733, 746-47 (9th Cir. 2015) (*en banc*) (dissolving a previously entered preliminary injunction compelling YouTube to take down copies of the film "Innocence of Muslims" and take all reasonable steps to prevent further uploads, which the *en banc* panel held had operated as a prior restraint), *citing Alexander v. United States*, 509 U.S. 544, 550 (1993) ("Temporary restraining orders and permanent injunctions—i.e., court orders that

for copyright infringement based on: (1) transmitting, routing, and providing connections to infringing material (the "routing" limitation, or what the statute refers to as "transitory digital network communications");[5] (2) system caching;[6] (3) information stored at the direction of a user (the "user storage" limitation);[7] or (4) linking or referring users to infringing material (the "information location tools" limitation).[8] It also creates a broad exemption from liability that could arise under any legal theory of law for disabling access to or removing in good faith allegedly infringing material (i.e., for taking down material, as a service provider is required to do to benefit from the liability limitations).[9]

For sites or services that host user generated content, the *user storage* and *information location tools* liability limitations will be the most important ones to consider. Service providers also should evaluate whether to comply with the procedures for counter notifications, which is not required but provides a mechanism for addressing user complaints if material is taken down in error (and provides an exemption from liability for wrongful takedowns). The first two limitations (routing and system caching) limit the risk of inadvertent liability that theoretically could arise simply by virtue of the way the Internet operates, where temporary copies of Internet transmissions and backup copies frequently are made.[10] The DMCA only limits a service provider's liability as of the date the service provider began complying with the statute.[11]

For the user storage and information location tools liability

---

actually forbid speech activities—are classic examples of prior restraints."); *supra* § 4.13[1].

[5]*See supra* § 4.12[4].

[6]*See supra* § 4.12[5].

[7]*See supra* § 4.12[6].

[8]*See supra* § 4.12[7].

[9]*See supra* § 4.12[8].

[10]*See supra* § 4.12.

[11]*See, e.g.*, *Perfect 10, Inc. v. CCBill, LLC*, 340 F. Supp. 2d 1077, 1092 (C.D. Cal. 2004) (holding that defendant Internet Key was ineligible for the DMCA liability limitations for acts of infringement that occurred prior to August 21, 2002, when it first implemented and distributed to clients its policy of terminating repeat infringers), *aff'd in part on other grounds,* 488 F.3d 1102 (9th Cir.), *cert. denied*, 522 U.S. 1062 (2007); *see also, e.g., Oppenheimer v. Allvoices, Inc.*, No. C 14–00499 LB, 2014 WL 2604033, at *6 (N.D. Cal. June 10, 2014) (holding the DMCA inapplicable to conduct

limitations, the term *service provider* is broadly defined and will include virtually all entities that host or provide links to user generated content, including websites, blogs, social networks, user generated content (UGC) sites, search engines and even potentially employers.[12] A narrower definition applies to the transitory digital network communications limitation, but that limitation applies to network transmissions and is unlikely to arise in a suit over user generated content.[13]

To qualify for any of the safe harbors, a service provider must satisfy the threshold prerequisites applicable to each of the four liability limitations,[14] as well as additional specific requirements applicable to a given safe harbor.

A service provider must accommodate and not interfere with *standard technical measures*[15] and adopt, reasonably implement, and inform subscribers and account holders[16] of a policy of terminating the accounts or subscriptions of repeat infringers in appropriate circumstances. For the user storage limitation (and potentially the information location tools[17] and caching[18] safe harbors), a service provider also must designate an agent to receive a special type of statutory demand letter called a *notification of claimed infringement* (referred to in this treatise as a *notification*, or more

---

that pre-dated the defendant's registration of its DMCA agent with the U.S. Copyright Office, in ruling on a motion to dismiss); *BWP Media USA Inc. v. Hollywood Fan Sites LLC*, 115 F. Supp. 397, 400-01 (S.D.N.Y. 2015) (citing *Oppenheimer* approvingly for the proposition that "[a] service provider cannot retroactively qualify for the safe harbor for infringements occurring before the proper designation of an agent under the statute" and holding that "§ 512(c) makes clear that it contemplates two parallel sources—the provider's website and the USCO directory—where each service provider's DMCA agent information is readily available to the public. For a service provider to fulfill only one of these two requirements is insufficient."); *supra* § 4.12[9][A] (collecting cases on registration as the start time for DMCA protection and criticizing the rule).

[12]*See* 17 U.S.C.A. § 512(k); *supra* § 4.12[2].

[13]*See supra* § 4.12[2].

[14]*See supra* § 4.12[3].

[15]*See supra* § 4.12[3].

[16]Not every type of service will have subscribers or account holders. Many services treat users as though they were subscribers or account holders to avoid any question about their entitlement to the safe harbor.

[17]*See supra* § 4.12[7] (analyzing whether a DMCA must be designated to qualify for the information location tools liability limitation).

[18]*See supra* § 4.12[5].

colloquially as a *DMCA notice*) and expeditiously disable access to or remove material or activity (or links) identified as infringing in substantially complying notifications.[19] Failing to respond to a notification may make a service provider ineligible for the safe harbor.[20] Religiously taking down material in response to substantially complying notifications, however, will not alone entitle a service provider to the benefits of the user storage safe harbors.

To take advantage of the user storage safe harbor, a service provider further must disable access to or remove material, even in the absence of a notification, if it has actual knowledge of infringing activity or is "aware of facts or circumstances from which infringing activity is apparent . . . ," which in the legislative history is explained as material that raises a "red flag."[21] Case law makes clear that knowledge or awareness must be of specific files or activity, not generalized knowledge that a site or service may be used for infringement.[22] Knowledge or awareness are judged by objective and subjective criteria, based on evidence such as internal emails or other messages that reflect knowledge or awareness of particular files at issue in a lawsuit (if not removed, once that knowledge or awareness is obtained). Whether a service provider has actual knowledge turns on whether it " 'subjectively' knew of specific infringement, while the red flag provision turns on whether the provider was subjectively aware of facts that would have made the specific infringement 'objectively' obvious to a reasonable

---

[19]*See supra* § 4.12[9].

[20]*See, e.g., Ellison v. Robertson*, 357 F.3d 1072 (9th Cir. 2004) (finding a triable issue of fact on the question of whether AOL satisfied the requirements of section 512(i) and therefore was entitled to limit its liability under the DMCA in a case where it failed to receive a notification, and therefore took no action, due to its own error).

[21]*See supra* § 4.12[6].

[22]*See, e.g., Capitol Records, LLC v. Vimeo, LLC*, 826 F.3d 78, 93 (2d Cir. 2016); *Viacom Int'l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 30–32 (2d Cir. 2012); *Ventura Content, Ltd. v. Motherless, Inc.*, 885 F.3d 597, 609-10 (9th Cir. 2018); *Mavrix Photographs, LLC v. LiveJournal, Inc.*, 873 F.3d 1045, 1057 (9th Cir. 2017); *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1021–23 (9th Cir. 2013); *BWP Media USA, Inc. v. Clarity Digital Group, LLC*, 820 F.3d 1175, 1182 (10th Cir. 2016) (quoting *Shelter Capital* with approval on this point); *supra* § 4.14[6][C] (extensively analyzing knowledge and red flag awareness).

person."[23] The Ninth Circuit suggested in *dicta* that notice from a third party may create red flag awareness, although the statute makes clear that knowledge or awareness may not be inferred from a defective notification sent by a copyright owner.[24] A service provider has no obligation to proactively search for infringing material.[25] At the same time, knowledge or awareness may be established through evidence of willful blindness.[26]

---

[23]*Viacom Int'l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 31 (2d Cir. 2012); *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1025 (9th Cir. 2013) (quoting *Viacom v. YouTube*). The Ninth Circuit has underscored that "whether 'the specific infringement' is 'objectively obvious to a reasonable person' may vary depending on the facts proven by the copyright holder in establishing liability." *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1026 n.15 (9th Cir. 2013).

[24]*See* 17 U.S.C.A. § 512(c)(3)(B)(i) (stating that neither knowledge nor awareness may be inferred from a notice that fails to meet statutory requirements); *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1024–25 (9th Cir. 2013). In *Shelter Capital,* UMG had argued that Veoh had red flag awareness of infringing material based on emails sent to Veoh executives by copyright owners, including an email sent by Disney's CEO to Michael Eisner, a Veoh investor, stating that unauthorized copies of the movie *Cinderella III* and various episodes from the television show *Lost* were posted on Veoh's site. The Ninth Circuit panel explained that "[i]f this notification had come from a third party, such as a Veoh user, rather than from a copyright holder, it might meet the red flag test [assuming the material was not taken down in response to the notice] because it specified particular infringing material. As a copyright holder, however, Disney is subject to the notification requirements in § 512(c)(3), which this informal email failed to meet." *Id.* (footnote omitted).

[25]17 U.S.C.A. § 512(m); *see also UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1022 (9th Cir. 2013).

[26]*See Capitol Records, LLC v. Vimeo, LLC,* 826 F.3d 78, 98-99 (2d Cir. 2016) (finding no willful blindness in that case); *Viacom Int'l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 35 (2d Cir. 2012) (holding that knowledge or awareness may be established by evidence of willful blindness, which the court characterized as a deliberate effort to avoid guilty knowledge); *Columbia Pictures Industries, Inc. v. Fung*, 710 F.3d 1020, 1043 (9th Cir. 2013) (explaining that "inducing actions"—or conduct deemed to induce copyright infringement—were relevant to the court's determination that the defendant had red flag awareness); *see also UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1023 (9th Cir. 2013) (citing *Viacom v. YouTube* for the proposition that "a service provider cannot willfully bury its head in the sand to avoid obtaining . . . specific knowledge."); *BWP Media USA, Inc. v. Clarity Digital Group, LLC*, 820 F.3d 1175, 1182 (10th Cir. 2016) (holding that a service provider was not willfully blind to infringement); *supra* § 4.12[6][C].

Whether and to what extent a service provider can lose DMCA protection for an employee's failure to properly implement DMCA procedures or for their misconduct is an evolving issue. The Second Circuit held that the mere fact that an employee saw a video on his employer's site that included substantially all of a recording of recognizable copyrighted music (or posted a comment, added it to a channel or "liked" the video), was insufficient to sustain the copyright owner's burden of proving that the service provider had either actual knowledge or red flag awareness of the infringement because that fact alone did not account for whether the music was in fact recognized by the employee as infringing.[27] The Tenth Circuit has held that a service provider does not automatically lose DMCA protection for the infringing activity of employees where the employees were merely acting as users of the service.[28] The Ninth Circuit looks to agency law for both employees and unpaid moderators to determine actual or apparent authority, with the further wrinkle that beyond knowledge or red flag awareness potentially attributable to a service provider, the Ninth Circuit has suggested that material may not even qualify as "stored at the direction of a user" if it is reviewed prior to upload, leaving potentially a factual question in some cases whether the material was stored by the employee or moderator or at the direction of the user.[29] In other cases, whether employee knowledge or misconduct could be attributed to the service provider would likely turn on traditional principles of respondeat superior, and whether the employee's acts or omissions were undertaken within the scope of his or her employment.[30]

Eligibility for the user storage liability limitation also

---

[27]*Capitol Records, LLC v. Vimeo, LLC*, 826 F.3d 78, 96-98 (2d Cir. 2016). The Second Circuit held that once a service provider establishes its prima facie entitlement to the DMCA safe harbor, the burden shifts to the copyright owner to prove disqualifying conditions such as actual knowledge or red flag awareness. *See id.* at 94-98.

[28]*BWP Media USA, Inc. v. Clarity Digital Group, LLC*, 820 F.3d 1175, 1181 (10th Cir. 2016).

[29]*See Mavrix Photographs, LLC v. LiveJournal, Inc.*, 873 F.3d 1045 (9th Cir. 2017); *see generally supra* § 4.12[6][A] (analyzing the case and criticizing this holding as inconsistent with the framework of the DMCA and its legislative history because, among other things, the statute creates a safe harbor that broadly protects service providers for material stored *at the direction of a user*, not literally material stored directly by users themselves).

[30]*See generally supra* § 4.12.

requires a showing that a defendant 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.[31] To benefit from the safe harbor, a service provider may not have *both* a financial interest and the right and ability to control. Service providers with a financial interest, but no right and ability to control, and those that have a right and ability to control but no financial interest, are eligible for the safe harbor.[32] Needless to say, a service provider with neither a financial interest nor the right and ability to control will also be eligible.

The financial interest prong has been construed in the Ninth Circuit as requiring a showing that " 'the infringing activity constitutes a draw for subscribers, not just an added benefit' "[33]

Right and ability to control within the meaning of the DMCA requires a higher showing than what would be required to establish common law vicarious liability—*i.e.,* more than merely the general ability to block access or remove content.[34] Prior disagreement between the Second and Ninth Circuits over what constitutes right and ability to control has been resolved in favor of the Second Circuit's in-

---

[31] 17 U.S.C.A. § 512(c)(1)(B); *supra* § 4.12[6][D].

[32] *See supra* § 4.12[6][D].

[33] *Columbia Pictures Industries, Inc. v. Fung*, 710 F.3d 1020, 1044-45 (9th Cir. 2013) (finding a financial interest where the defendant earned advertising revenue from ads marketed based on the popularity of infringing material on his sites, where approximately 90-96 percent (or perhaps slightly less) of the content on his sites was infringing and where the defendant actively induced infringement by users of the service); *Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102, 1117–18 (9th Cir.) (finding that evidence that the service provider hosted, for a fee, websites that contained infringing material inadequate to establish the requisite financial benefit based on the literal language of the legislative history), *cert. denied*, 522 U.S. 1062 (2007); *Ellison v. Robertson*, 357 F.3d 1072, 1079 (9th Cir. 2004) (quoting legislative history) (holding that "financial interest" under the DMCA should be found where "there is a causal relationship between the infringing activity and any financial benefit a defendant reaps . . . ;" affirming the finding that there was no financial interest based on inadequate proof that "customers either subscribed because of the available infringing material or cancelled subscriptions because it was no longer available."); *see generally supra* § 4.12[6][D].

[34] *See, e.g.*, *Viacom Int'l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 37-38 (2d Cir. 2012); *CoStar Group, Inc. v. LoopNet, Inc.*, 373 F.3d 544, 555 (4th Cir. 2004); *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1026-31 (9th Cir. 2013); *supra* § 4.12[6][D].

terpretation that right and ability to control does not presuppose knowledge of specific infringing activity.[35] According to the Second Circuit, what is required is "something more than the ability to remove or block access to materials posted on a service provider's website."[36] That "something more" is understood in the Second and Ninth Circuit to involve exerting "substantial influence" on the activities of users, which may include high levels of control over user activities or purposeful conduct.[37] Right and ability to control and financial interest are analyzed in section 4.12[6][D].

At least for purposes of the user storage limitation (and presumably for the information location tools safe harbor, to the extent applicable service providers have account holders and subscribers), the Ninth Circuit has held that in evaluating a service provider's compliance with the threshold requirement that a service provider adopt, notify subscribers about and implement a policy of terminating "repeat infringers" in "appropriate circumstances," a court must also consider the service provider's compliance with third-party notifications and response to all instances where it had actual knowledge or red flag awareness of infringement (not merely how it acted in responding to the plaintiff's own works), on the theory that a service provider may not be reasonably implementing a policy of terminating repeat infringers in appropriate circumstances if it is not, in the first instance, adequately keeping track of who is an infringer. Needless to say, this standard potentially puts at issue a service provider's entire operations any time it is sued (and also potentially may make it more difficult to obtain summary judgment on a service provider's entitlement to the DMCA defense in certain cases).[38]

The statute affords service providers significant flexibility in designing and implementing a repeat infringer policy.

---

[35]*See Viacom Int'l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 36 (2d Cir. 2012) (disagreeing with the original Ninth Circuit opinion from 2011 in *Shelter Partners*); *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1026-31 (9th Cir. 2013) (following *Viacom v. YouTube*).

[36]*Viacom Int'l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 38 (2d Cir. 2012), *quoting Capitol Records, Inc. v. MP3Tunes, LLC*, 821 F. Supp. 2d 627, 645 (S.D.N.Y. 2011).

[37]*See Viacom Int'l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 38 (2d Cir. 2012); *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1030 (9th Cir. 2013).

[38]*See supra* § 4.12[18] (discovery issues in DMCA litigation).

Termination need only be "in appropriate circumstances," not automatically. Similarly, the term *repeat infringer* is not defined in the DMCA. As a practical matter, however, service providers may be better off adopting a stricter policy than the law requires because it will be easier for the service provider to obtain summary judgment than if it liberally exercises its discretion to determine what *appropriate circumstances* might be, which could raise factual disputes in individual cases that could preclude summary judgment.

What constitutes an *infringer* should not be defined too narrowly. The Second Circuit has held that a policy that treated uploaders as infringers for purposes of a DMCA repeat infringer policy, but did not consider downloads of infringing material intended for personal use to be infringing, was unreasonable.[39]

District courts in Los Angeles and New York have approved a "three strikes" policy for terminating repeat infringers.[40] A more conservative approach would be to treat a repeat infringer as literally anyone who has been the

---

[39]*See EMI Christian Music Group, Inc. v. MP3Tunes, LLC*, 844 F.3d 79, 88-89 (2d Cir. 2016).

[40]*See Capitol Records, LLC v. Vimeo, LLC*, 972 F. Supp. 2d 500, 536–37 (S.D.N.Y. 2013), *aff'd in part, rev'd in part on other grounds*, 826 F.3d 78 (2d Cir. 2016); *Viacom Int'l Inc. v. YouTube, Inc.*, 718 F. Supp. 2d 514 (S.D.N.Y. 2010), *aff'd in relevant part on other grounds*, 676 F.3d 19, 40–41 (2d Cir. 2012); *UMG Recordings, Inc. v. Veoh Networks Inc.*, 665 F. Supp. 2d 1099, 1118 (C.D. Cal. 2009), *aff'd on other grounds sub nom. UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006 (9th Cir. 2013); *Perfect 10, Inc. v. CCBill, LLC*, 340 F. Supp. 2d 1077, 1094 n.12 (C.D. Cal. 2004), *aff'd in part on other grounds*, 488 F.3d 1102 (9th Cir.), *cert. denied*, 522 U.S. 1062 (2007); *see generally supra* § 4.12[3][B].

In *YouTube*, the district court also rejected Viacom's argument that YouTube did not reasonably implement its repeat infringer policy because it treated as only one strike: (1) a single DMCA takedown notice identifying multiple videos; and (2) multiple takedown notices identifying videos uploaded by a user received by YouTube within a two-hour period.

The district court likewise discounted Viacom's argument that YouTube's repeat infringer policy was not reasonably implemented because YouTube only counted DMCA notices; it did not account for videos automatically removed by Audible Magic content filters. These aspects of the district court's ruling were not addressed in the Second Circuit's opinion, which focused narrowly on the issue of whether YouTube's provision of a search tool only to business partners, and not plaintiffs, meant that it had failed to reasonably implement its repeat infringer policy (which the appellate court concluded it had not).

In *Vimeo*, the district court expressly approved of a service provider's policy of treating notifications received within a three-day pe-

subject of a prior DMCA notification. Indeed, some service providers will terminate some users based on the first notice received when it is apparent that the user is engaged in willful infringement. On the other hand, appropriate circumstances may exist for not terminating a user upon receipt of a second or even third DMCA notice where, for example, the prior notice was sent in error or was the subject of a counter notification not thereafter challenged by a copyright owner or where the user is unlikely to infringe in the future (such as where notifications addressed material that was posted based on a mistaken view of fair use, which has since been corrected).

The granular details of the policy need not be posted on a site or otherwise publicized—and indeed it is advisable not to do so or the policy could be construed as creating a quasi-contractual obligation of the service provider and any errors in implementation could be viewed negatively by a judge or jury. To comply with the requirement that a service provider notify subscribers and account holders of the policy it is sufficient to simply state in Terms of Use, ISP service contracts or elsewhere that the site or service has a policy of terminating repeat infringers in appropriate circumstances, tracking the statutory language exactly but saying no more.

To show compliance with the obligation that material be removed in response to knowledge or "red flag" awareness, service providers should keep adequate records and ensure that they are stored in a manner that would be admissible as business records.[41] Service providers also should keep records showing that users were in fact terminated as repeat infringers. If a site or service has never terminated users as repeat infringers and never removed material on its own initiative (but only in response to DMCA notifications) it may have difficulty proving its entitlement to DMCA protection if it hosts a user generated content (UGC) site where infringement plainly occurs. Every piece of potentially infringing material reviewed by site employees potentially could become at issue in a lawsuit. While it is often very difficult to discern whether material in fact is authorized or infringing, a site that never removes material based on "red flag" awareness

---

riod as a single strike. *See Capitol Records, LLC v. Vimeo, LLC*, 972 F. Supp. 2d 500, 514–16 (S.D.N.Y. 2013), *aff'd in part rev'd in part, on other grounds*, 826 F.3d 78 (2d Cir. 2016).

[41] *See generally infra* § 58.02.

may appear less compliance-oriented to a judge or jury than one that makes a good faith effort to comply with the statutory requirements of the DMCA, even if in particular cases it may have omitted to remove material that the trier of fact would consider raises a red flag. A service provider that has never removed material on its own initiative may have a harder time defending why it did not remove particular examples cited by a copyright owner in litigation.

The law and policy options for service provider adoption, implementation and notice of a repeat infringer policy,[42] responding to notifications,[43] actual knowledge and "red flag" awareness[44] are analyzed extensively in section 4.12.

Where they do not otherwise have actual knowledge or "red flag" awareness, service providers have no obligation to act unless they receive a substantially complying notification (and neither knowledge nor awareness may be inferred from a notification that is not substantially complying).[45] Hence, a service provider may not be successfully sued for copyright infringement if it was not first provided the opportunity to respond to a substantially complying notification (assuming that the service provider meets the other statutory requirements to qualify for the applicable safe harbor). In addition, a copyright owner may not effectively shift its burden of searching for infringing material and providing notifications to service providers by sending a notice that purports to ask the service provider prospectively to remove material not then on its site or service.[46]

To benefit from the related exemption from liability for removing material stored by subscribers, service providers must also respond to counter notifications which may be

---

[42] *See supra* § 4.12[3].

[43] *See supra* §§ 4.12[6], 4.12[9].

[44] *See supra* § 4.12[6][B].

[45] *See* 17 U.S.C.A. § 512(c)(3)(B)(i). Where a notification is deficient but nonetheless substantially complies with the requirements for identifying the infringed work and the infringing material and includes sufficient contact information to allow the service provider to contact the complainant, however, the service provider must attempt to do so or "tak[e] other reasonable steps to assist" in obtaining a substantially complying notification before it may benefit from this provision. *See* 17 U.S.C.A. § 512(c)(3)(B)(ii); *see generally supra* §§ 4.12[6][C], 4.12[9]B].

[46] *Hendrickson v. Amazon.com, Inc.*, 298 F. Supp. 2d 914 (C.D. Cal. 2003); *see generally supra* §§ 4.12[1], 4.12[9] (analyzing a service provider's obligations in response to notifications).

directed to their agents by subscribers whose content was removed (or access disabled) in response to a notification.[47] When a substantially complying counter notification is received, a service provider must pay close attention to statutory time periods and either restore access to or re-post content that previously had been removed (if a copyright owner fails to timely respond to a counter notification), or take no further action, and leave the material offline (if the copyright owner timely provides evidence to the service provider that it has filed suit against the subscriber or account holder).[48] Some sites and services consider it to be good for public relations or on principle to afford users the opportunity to challenge DMCA notifications, which potentially could have been sent in error or address material that could be licensed or permissible as a fair use. Indeed, providing users with a mechanism to dispute notifications may help deflect any frustration that otherwise might be directed at the service provider when material that a user considers to be his or her own—such as a vacation video that includes unauthorized music—is removed. As a practical matter, however, service providers may not need the added protection provided by the procedures for counter notifications and may find it burdensome or expensive to comply with them.

The DMCA creates a broad exemption when service providers take down material on their own initiative—for example when they acquire actual knowledge or "red flag" awareness of infringement. Complying with counter notification procedures will only provide an additional measure of protection in cases where material is removed in response to a DMCA notification and the subscriber or account holder objects by filing a counter notification. In those limited circumstances, a service provider must restore material that was taken down and follow the requirements of the statute or it will not enjoy an exemption from liability in a suit brought by an account holder or subscriber for having taken down the material. In practice, however, suits by subscribers or account holders are rare. Moreover, because, by definition, account holders and subscribers should have privity of contract with a service provider, liability for taking down material in response to a DMCA notification may be limited by the service provider's contract with its subscribers and

---

[47] *See supra* § 4.12[13].

[48] *See supra* § 4.12[9][C].

account holders.[49] Service providers also potentially could be exempt from liability for removing material in response to a DMCA notification under the Good Samaritan Exemption to the Telecommunications Act of 1996 (also known as the Communications Decency Act, or CDA).[50]

Whether a service provider complies with the procedures for counter notifications is a matter of choice based on the costs of compliance, its own risk assessment and customer relations. In earlier days, many sites or services considered the DMCA to be burdensome and expensive to comply with.[51] Today, compliance with the user storage liability and information location tools limitations of the DMCA is widely seen as almost essential for any site or service that allows users to post, store or transmit material and also may be required by many insurers of interactive sites and services.

Sites and services that host user generated content should comply with the UGC Principles agreed upon by a group of service providers, technology companies and motion picture and television companies.[52] By doing so, a service provider will insulate itself from liability to any of the content owners that have signed on to the Principles and agreed not to sue compliant sites. The Principles require undertakings beyond what the DMCA literally requires—such as the use of filtering technologies—but these practices will better insulate a service provider from liability even to non-signatories to the Principles and minimize risk in an area where almost all of the case law has been decided by only two circuits. The UGC Principles have also helped shape "best practices" by UGC Sites, leaving a site that fails to comply exposed in litigation to being viewed as an outlier, rather than a compliance-oriented company (which can be especially important in cases where mistakes in implementation of a DMCA program have been made and a service provider may need the benefit of the doubt from a judge or jury).

---

[49] *See supra* chapters 21 (click through and other unilateral contracts), 22 (Terms of Use) and 23 (ISP contracts). Whether and to what extent Service Provider agreements will be deemed enforceable is analyzed in sections 21.03 and 21.04. DMCA compliance is separately addressed in sections 4.12 and 22.05[2][A].

[50] 47 U.S.C.A. § 230(c); *see generally supra* §§ 4.12[8], 37.05, 49.04.

[51] *See supra* §§ 4.12[1], 4.12[13].

[52] *See supra* § 4.12[17].

49.05[3] Direct, Contributory, Vicarious and Inducing Copyright Infringement

49.05[3][A] In General

Where the DMCA does not otherwise insulate a service provider from liability for damages and attorneys' fees for user generated content, a site or service may risk exposure for direct liability, contributory infringement, vicarious liability or inducing copyright infringement, which are analyzed extensively in section 4.11. As noted earlier, most suits against legitimate sites and services over user generated content are likely to focus on contributory infringement and vicarious liability, although claims for inducement and direct liability also may be alleged.

49.05[3][B] Direct Liability

The Copyright Act is a strict liability statute and therefore, at least in theory, direct liability could be imposed simply because infringing content was stored or posted on, or transmitted from, a defendant's server. Since 1995, however, every court that has considered the issue has followed *Religious Technology Center v. Netcom On-Line Communication Services, Inc.*[1] in ruling that an online service may not be held directly liable for infringing material posted by a user absent some *volitional act* or *direct action* to facilitate the underlying act of infringement.[2] Direct liability is analyzed in section 4.11[2].

[Section 49.05[3][B]]

[1]*Religious Technology Center v. Netcom On-Line Communication Services, Inc.*, 907 F. Supp. 1361 (N.D. Cal. 1995).

[2]*See Religious Technology Center v. Netcom On-Line Communication Services, Inc.*, 907 F. Supp. 1361, 1370 (N.D. Cal. 1995); *see also, e.g.*, *Cartoon Network LP, LLLP v. CSC Holdings, Inc.*, 536 F.3d 121, 131 (2d Cir. 2008) (holding that a company could not be held directly liable for its provision of a DVR service because "the operator . . . , the person who actually presses the button to make the recording, supplies the necessary element of volition, not the person who manufactures, maintains, or, if distinct from the operator, owns the machine."), *cert. denied,* 557 U.S. 946 (2009); *Parker v. Google, Inc.*, 242 F. App'x 833 (3d Cir. 2007) (affirming dismissal, in an unreported decision, of plaintiff's claim alleging that part of his work had been copied without authorization in a Usenet post, where the plaintiff failed to allege any volitional conduct on the part of Google in archiving Usenet postings); *CoStar Group, Inc. v. LoopNet, Inc.*, 373 F.3d 544 (4th Cir. 2004); *BWP Media USA, Inc. v. T&S Software Associates, Inc.*, 852 F.3d 436, 438-44 (5th Cir.) (affirming summary judgment for T & S Software Associates, an internet service provider, holding that it was

49.05[3][C] Contributory Infringement

Liability for contributory copyright infringement may be imposed where a person or entity "induces, causes or materially contributes to the infringing conduct of another . . . ."[1] A *prima facie* case of contributory infringement is presented

---

not directly liable for hosting an internet forum on which third-party users posted images that allegedly infringed copyrights owned by plaintiffs), *cert. denied*, 138 S. Ct. 236 (2017); *Perfect 10, Inc. v. Giganews, Inc.*, 847 F.3d 657, 666–67 (9th Cir. 2017) (affirming dismissal and summary judgment for defendants on plaintiff's direct infringement claims brought against ISPs that provided access to the USENET and a software program to be able to view USENET content, which, among many other things, plaintiffs claimed included infringing copies of its photos); *Fox Broadcasting Co. v. Dish Network LLC*, 747 F.3d 1060, 1066-68 (9th Cir. 2014) (applying *Cartoon Network* in holding that a cable company that provided technology to its subscribers that they could use to make copies was not likely to be held directly liable because Dish itself did not make the copies and direct liability requires a showing of causation—or evidence of "copying by the defendant"); *Field v. Google Inc.*, 412 F. Supp. 2d 1106, 1115 (D. Nev. 2006) (holding Google not liable for caching plaintiff's website articles as part of its automatic caching of the Internet, where the plaintiff had indicated in the metatags of his website that he wanted to be crawled by Google; "Google is passive in this process . . . . Without the user's request the copy would not be created and sent to the user, and the alleged infringement at issue in this case would not occur. The automated, nonvolitional conduct by Google in response to a user's request does not constitute direct infringement . . . ."); *Playboy Enterprises, Inc. v. Russ Hardenburgh, Inc.*, 982 F. Supp. 503 (N.D. Ohio 1997); *Sega Enterprises Ltd. v. MAPHIA*, 948 F. Supp. 923, 932 (N.D. Cal. 1996) (following *Netcom*); *Marobie-FL, Inc. v. National Ass'n of Fire Equipment Distributors*, 983 F. Supp. 1167, 1172 (N.D. Ill. 1997) ("Direct infringement does not require any particular state of mind"); *Ellison v. Robertson*, 189 F. Supp. 2d 1051, 1057 (C.D. Cal. 2002) (following *Netcom* in holding that "AOL's role in the infringement as a passive provider of Usenet access to AOL users cannot support direct copyright infringement liability" in a case involving an eBook posted to a newsgroup), *aff'd in part and rev'd in part*, 357 F.3d 1072 (9th Cir. 2004); *Perfect 10, Inc. v. Cybernet Ventures, Inc.*, 213 F. Supp. 2d 1146, 1168 (C.D. Cal. 2002) (following *Netcom* for the proposition that "defendants must actively engage in one of the activities recognized in the Copyright Act" before direct liability could be imposed on a site or service); *see generally supra* § 4.11[2] (analyzing the issues at greater length).

[Section 49.05[3][C]]

[1]*See, e.g., Sega Enterprises Ltd. v. MAPHIA*, 857 F. Supp. 679, 686 (N.D. Cal. 1994); *see also, e.g.*, *Playboy Enterprises, Inc. v. Russ Hardenburgh, Inc.*, 982 F. Supp. 503 (N.D. Ohio 1997); *Sega Enterprises Ltd. v. MAPHIA*, 948 F. Supp. 923 (N.D. Cal. 1996); *Sega Enterprises Ltd. v. Sabella,* Case No. C 93-04260 CW, 1996 WL 780560 (N.D. Cal. Dec. 18, 1996).

where a plaintiff alleges: (1) direct infringement by a third party; (2) knowledge by the defendant that third parties were directly infringing; and (3) substantial participation by the defendant in the infringing activities.[2]

Except where a defendant's own conduct is at issue, site owners and service providers most frequently risk liability for contributory infringement where they receive actual notice about an alleged act of infringement and thereafter take no action to end it. Even though in many cases a cease and desist letter or email may not actually provide enough information to evaluate whether a work in fact is infringing (i.e., whether the two works really are substantially similar or whether the alleged infringer may have a valid fair use defense, for example), there is authority for the proposition that the failure to even investigate an alleged act of infringement in response to a notice at least creates a factual dispute that precludes the entry of summary judgment on a plaintiff's claim for contributory infringement.[3] In this regard, the standard for imposing contributory copyright infringement is somewhat easier to meet than for contributory trademark infringement[4] (or by extension potentially other claims for contributory infringement of intellectual property rights).

In *Perfect 10, Inc. v. Amazon.com, Inc.*[5] the Ninth Circuit held that liability for contributory infringement could be imposed on defendant search engines if they had knowledge that infringing images were available using their search engine, could take simple measures to prevent further damage to the plaintiff's copyrighted works, and failed to take such steps.[6]

The *Perfect 10* articulation of the grounds on which li-

---

[2]*UMG Recordings, Inc. v. Bertelsmann AG*, 222 F.R.D. 408 (N.D. Cal. 2004).

[3]*See, e.g., Religious Technology Center v. Netcom On-Line Communication Services, Inc.*, 907 F. Supp. 1361, 1374 (N.D. Cal. 1995) (holding that a service provider's acknowledged receipt of a letter demanding that certain content be removed created a material factual dispute precluding summary judgment on the issue of whether it was contributorily liable for a user's act of infringement, while also expressing skepticism in *dicta* that liability could be imposed on such grounds); *see generally supra* § 4.11.

[4]*See infra* § 49.06[3].

[5]*Perfect 10, Inc. v. Amazon.com, Inc.*, 508 F.3d 1146 (9th Cir. 2007); *see generally supra* § 4.11[5].

[6]508 F.3d at 1172.

ability may be imposed does not supplant the traditional test for contributory infringement; it merely represents an alternative formulation that could allow for a finding of liability where a defendant could have, but failed to take simple steps to prevent or deter infringement once it obtained specific knowledge of acts of infringement.

Whichever formulation applies, courts in the Ninth Circuit and Southern District of New York have held that, as with knowledge or awareness under the DMCA, knowledge for purposes of imposing liability for contributory infringement must be of specific infringing files or activity; generalized knowledge will not suffice.[7]

By contrast, in *Flava Works, Inc. v. Gunter*,[8] Judge Posner of the Seventh Circuit criticized what he characterized as the traditional test for contributory infringement and its various articulations, preferring instead the formulation that contributory infringement may be imposed based on "personal conduct that encourages or assists the infringement . . . ."[9] Judge Posner explained in *dicta* that *material contribution* in the context of what he called "the conventional definition of contributory infringement" invokes "common law notions of remoteness that limit efforts to impose li-

---

[7] *See, e.g.*, *Luvdarts, LLC v. AT&T Mobility, LLC*, 710 F.3d 1068, 1072 (9th Cir. 2013) (affirming that the plaintiff did not state a claim for contributory infringement against mobile phone carriers over the alleged infringement of their users in forwarding text messages containing original content without authorization to do so because a plaintiff must allege "more than a generalized knowledge . . . of the possibility of infringement."); *Perfect 10, Inc. v. Amazon.com, Inc.*, 508 F.3d 1146, 1172 (9th Cir. 2007) ("a computer system operator can be held contributorily liable if it 'has *actual* knowledge that *specific* infringing material is available using its system . . .' "; *citing A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004, 1022 (9th Cir. 2001) (emphasis in original)); *Wolk v. Kodak Imaging Network, Inc.*, 840 F. Supp. 2d 733, 751 (S.D.N.Y. 2012) (holding that for liability to attach, actual or imputed knowledge must be based on specific and identifiable infringements of individual items, not a general awareness of infringement), *aff'd mem.*, 569 F. App'x 51 (2d Cir. 2014).

[8] *Flava Works, Inc. v. Gunter*, 689 F.3d 754 (7th Cir. 2012).

[9] *Flava Works, Inc. v. Gunter*, 689 F.3d 754, 757 (7th Cir. 2012), *quoting Matthew Bender & Co. v. West Publishing Co.*, 158 F.3d 693, 706 (2d Cir. 1998).

Both *Perfect 10* and *Flava Works* involved suits over in-line links. The Seventh Circuit in *Flava Works* took a different approach to the issue, and applied a different formulation of the test for contributory infringement, than the Ninth Circuit in *Perfect 10* court. *See supra* § 9.03[3][A] (analyzing both cases).

ability for speculative imaginings of possible causal connections."[10] In explaining what is *not* material, Judge Posner wrote that "[a]n injury will sometimes have a cascading effect that no potential injurer could calculate in deciding how carefully to act. The effect is clear in hindsight-but only in hindsight."[11]

Among other things, contributory infringement potentially may be imposed where a site or service offers cracker tools or other software or devices[12] that facilitate third-party acts of infringement or otherwise actively encourages infringing activity by its users.

Liability for contributory infringement, however, may not be imposed where a program, tool or technology has *substantial noninfringing uses*.[13]

The legal grounds on which contributory infringement may be imposed are analyzed in substantially greater detail in section 4.11[3].

49.05[3][D] Vicarious Infringement

Vicarious liability may be imposed where a defendant (1) has the right and ability to supervise a third-party's infringing activity, and (2) has a direct financial interest in it.[1] Based on pre-Internet case law developed on *terra firma*, site owners and service providers potentially may be held vicariously liable for acts of copyright infringement that they did not condone and may even have been unaware of. As a practical matter, however, judges and juries are often reticent about imposing liability under these circumstances. On the other hand, where a defendant appears to have acted

---

[10] *Flava Works, Inc. v. Gunter*, 689 F.3d 754, 759 (7th Cir. 2012).

[11] *Flava Works, Inc. v. Gunter*, 689 F.3d 754, 759 (7th Cir. 2012), *quoting BCS Services, Inc. v. Heartwood 88, LLC*, 637 F.3d 750, 755 (7th Cir. 2011).

[12] *See, e.g., Sega Enterprises Ltd. v. MAPHIA*, 948 F. Supp. 923 (N.D. Cal. 1996) (product that allowed BBS subscribers to convert videogame software from Sega's proprietary format to generic disks, where the games could be easily uploaded to the BBS).

[13] *See Sony Corp. of America v. Universal City Studios, Inc.*, 464 U.S. 417, 442 (1984); *Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd.*, 545 U.S. 913 (2005); *see generally supra* §§ 4.11[4], 4.11[7].

[Section 49.05[3][D]]

[1] *See, e.g., Fonovisa, Inc. v. Cherry Auction, Inc.*, 76 F.3d 259, 262 (9th Cir. 1996); *see generally supra* § 4.11[4].

improperly or turned a blind eye to obvious infringing activity, courts may stretch the technical requirements in order to impose vicarious liability.[2]

In *dicta* in *MGM Studios, Inc. v. Grokster*,[3] the U.S. Supreme Court stated the test somewhat differently in passing in a case that addressed contributory infringement and inducement, writing that a defendant "infringes vicariously by profiting from direct infringement while declining to exercise a right to stop or limit it."[4]

Depending which test is applied, the showing required to satisfy the financial interest prong of the test for vicarious liability in digital piracy cases may be low. Actually earning revenue is not necessarily required. In *A&M Records, Inc. v. Napster, Inc.*,[5] for example, the Ninth Circuit rejected the argument that Napster did not have a "financial interest" in its service because the Napster service was available without charge, holding that a "[f]inancial benefit exists where the availability of infringing material acts as a 'draw' for customers."[6] In addition, the court noted that Napster's future revenues were directly dependent on increasing its user base.

Whether charging a flat fee is enough to be deemed to have a financial interest has been somewhat confused in case law. In *Religious Technology Center v. Netcom On-Line Communication Service, Inc.*,[7] a seminal 1995 decision involving secondary liability for Internet service providers, the court had held that a service provider did *not* have a financial interest where it charged the same flat fee for

---

[2]These phenomena are discussed more extensively in section 4.11.

[3]*Metro-Goldwyn-Mayer Studios, Inc. v. Grokster Ltd.*, 545 U.S. 913 (2005).

[4]*MGM Studios Inc. v. Grokster, Ltd.*, 545 U.S. 930 (2005), *citing Shapiro, Bernstein & Co. v. H. L. Green Co.*, 316 F.2d 304, 307 (2d Cir. 1963); *see also, e.g.*, *Luvdarts, LLC v. AT&T Mobility, LLC*, 710 F.3d 1068, 1071 (9th Cir. 2013) (applying this formulation of the test in holding that mobile carriers did not have the right or ability to supervise the alleged infringement of their users in forwarding text messages containing original content without authorization to do so);

[5]*A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004 (9th Cir. 2001).

[6]*A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004, 1023 (9th Cir. 2001).

[7]*Religious Technology Center v. Netcom On-Line Communication Services, Inc.*, 907 F. Supp. 1361 (N.D. Cal. 1995); *see generally supra* § 4.11[8][B].

Internet access to all subscribers. In so ruling, however, District Court Judge Ronald Whyte relied on the lower court decision from 1994 in *Fonovisa, Inc. v. Cherry Auction, Inc.*,[8] in which the district court had held that a flea market owner did not have a financial interest in the infringing activities of certain participants at the flea market because all participants were charged the same flat fee. The Ninth Circuit, however, reversed that decision in 1996, holding that the swap meet owner *did* have a "direct financial interest" because it earned admission fees, concession stand sales and parking fees from infringing vendors, even though these same flat fees were charged to all vendors—not just those who were engaged in infringing activity. Subsequent case law has either followed *Fonovisa* in holding that a flat fee creates or financial interest or *Netcom* without regard to the fact that *Netcom* relied on the lower court opinion in *Fonovisa* that itself was reversed on appeal.[9] The difference between the two standards is analogous to the difference between general and specific causation in tort law.

In *Ellison v. Robertson*,[10] the Ninth Circuit held that merely providing Usenet access to subscribers was not sufficient to hold that AOL (which charged customers a flat monthly fee) had a financial interest in third-party acts of infringement over the Internet absent evidence that AOL attracted or retained subscribers because of the alleged acts of infringement or lost subscriptions because of its eventual obstruction of the infringement. Following *Napster*, the court applied the test of "whether the infringing activity constitutes a draw for subscribers, not just an added benefit."[11] This is also the test applied in many DMCA cases.[12]

Which standard is applied for evaluating financial interest may be outcome determinative.

While the financial interest prong may or may not be difficult to establish in cases involving legitimate services, in many digital piracy cases liability for vicarious liability frequently turns on the second prong—right and ability to

---

[8] *Fonovisa, Inc. v. Cherry Auction, Inc.*, 847 F. Supp. 1492, 1496 (E.D. Cal. 1994), *rev'd,* 76 F.3d 259, 263 (9th Cir. 1996).

[9] *See generally supra* § 4.11[4].

[10] *Ellison v. Robertson*, 357 F.3d 1072 (9th Cir. 2004).

[11] *Ellison v. Robertson*, 357 F.3d 1072, 1079 (9th Cir. 2004).

[12] *See supra* § 4.12[6][D].

control. The extent to which a site owner or service provider may be deemed to have the right and ability to control third-party acts of infringement in cyberspace may depend on the nature of the particular site or service and the conduct alleged.[13] Judge Lewis Kaplan of the Southern District of New York has suggested that although literal application of physical world standards may not be appropriate in cases involving digital technology, "the notion that the control must be substantial and have practical force . . . remains sound."[14]

In *A&M Records, Inc. v. Napster, Inc.*,[15] the Ninth Circuit found that Napster's reservation of the right to block access "for any reason whatsoever" in its terms of use constituted evidence that it had the right and ability to supervise the infringing conduct of its users.[16] Likewise, in *Arista Records, Inc. v. MP3Board, Inc.*,[17] Judge Sidney Stein of the Southern District of New York ruled that plaintiffs had raised a triable issue precluding summary judgment by presenting evidence that MP3Board could delete links from its database (and had done so with various links that pointed to pornographic, hate, hacker and warez sites).

In *MGM Studios, Inc. v. Grokster, Ltd.*,[18] the Supreme Court characterized the test for vicarious liability at one point in *dicta* as allowing for the imposition of liability when a defendant "infringes vicariously by profiting from direct in-

---

[13]This issue is addressed in further detail in sections 4.11[8][B] and 4.11[8][C]. Third-party liability for site owners and service providers generally is analyzed in this chapter and chapters 50 and 51.

[14]*Faulkner v. National Geographic Society*, 211 F. Supp. 2d 450, 473 (S.D.N.Y. 2002), *aff'd on other grounds*, 409 F.3d 25 (2d Cir. 2005).

[15]*A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004 (9th Cir. 2001).

[16]*See generally supra* § 4.11[9][F]. *Napster* was a case where the defendants were found to have had knowledge that their service would be used to exchange infringing music files and intentionally set up their service to limit their ability to control user conduct. This evidence of willfulness—both in the form of willful misconduct and willful ignorance—undoubtedly colored the panel's opinion. As a general proposition, it is questionable whether merely reserving a right in posted Terms and Conditions in fact should be treated as equivalent to actually having the ability to control third-party conduct. *See supra* § 4.11[4] (and the cases analyzed in that section).

[17]*Arista Records, Inc. v. MP3Board, Inc.,* 00 Civ. 4660 (SHS), 2002 WL 1997918 (S.D.N.Y. Aug. 29, 2002).

[18]*Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd.*, 545 U.S. 913 (2005).

fringement while declining to exercise a right to stop or limit it."[19] This articulation arguably differs in some respects from the standard applied in several of the cases discussed earlier in this section.

The vicarious liability doctrine also may be used to hold individuals liable for the infringing activities of entities in which they have a financial interest (effectively allowing plaintiffs to pierce the corporate veil in circumstances where such a remedy would not be available under state corporate law). For example, in *Playboy Enterprises, Inc. v. Webbworld, Inc.*,[20] the court imposed vicarious liability on some, but not all owners of a Texas LLC that operated a subscription website service where visual images automatically culled from Usenet postings were made available to paid subscribers. The court ruled that although all owners had a financial interest in the service's infringing activities, a passive investor who did not work at the site did not have the ability to control the LLC's conduct, whereas other owners who wrote or programmed the software used to select the images did and therefore were held vicariously liable. Individual and investor liability is analyzed more extensively in section 4.11[5].

Although not expressly addressed in the U.S. Supreme Court's decision in *MGM Studios, Inc. v. Grokster, Ltd.*,[21] claims for vicarious liability based on websites, services and technologies may, like claims for contributory infringement, be subject to the safe harbor recognized by the Supreme Court in that case where products (broadly defined) have *substantial noninfringing uses*.[22]

Vicarious liability is addressed in more substantial detail in section 4.11[4].

49.05[3][E] Inducement

Although historically inducement had been one of several alternative grounds on which contributory copyright in-

---

[19]545 U.S. at 930, *citing Shapiro, Bernstein & Co. v. H. L. Green Co.*, 316 F.2d 304, 307 (2d Cir. 1963).

[20]*Playboy Enterprises, Inc. v. Webbworld, Inc.*, 991 F. Supp. 543, 554 (N.D. Tex. 1997), *aff'd mem.*, 168 F.3d 486 (5th Cir. 1999); *see also Playboy Enterprises, Inc. v. Webbworld, Inc.*, 968 F. Supp. 1171, 1176–77 (N.D. Tex. 1997).

[21]*Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd.*, 545 U.S. 913 (2005).

[22]*See supra* §§ 4.11[5], 4.11[7].

fringement could be found,[1] the U.S. Supreme Court, borrowing from patent law, recognized a new form of copyright inducement claim in 2005 in *MGM Studios, Inc. v. Grokster, Ltd.*,[2] holding that one 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.[3] The Court explained that liability for inducement must be premised on "purposeful, culpable expression and conduct," not mere knowledge by a distributor of potential or actual infringing uses. The Court also clarified that "ordinary acts incident to product distribution, such as offering customers technical support or product updates" would not support liability for inducement in and of themselves, absent other evidence of purposeful, culpable expression or conduct. Further, in footnote 13, the Court explained that it is not merely the encouragement of infringement that will give rise to a claim. There must also be distribution of a tool intended for infringing use to give rise to a claim for inducing copyright infringement[4] or provision of a service.[5]

Subsequent cases have imposed liability on companies that had a high percentage of infringing content on their sites or services, actively encouraged users to engage in copyright infringement and failed to take simple measures to deter user infringement.[6]

[Section 49.05[3][E]]

[1]*See supra* § 49.05[3].

[2]*Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd.*, 545 U.S. 913 (2005); *see generally* Ian C. Ballon, "Digital Copyright Litigation After *MGM Studios, Inc. v. Grokster*," Mealey's Litig. Report, July 2005.

[3]545 U.S. at 936–37.

[4]The Court explained that while encouraging a particular consumer to infringe a copyright can give rise to secondary liability (presumably for contributory or vicarious infringement) for the infringement that results, "[i]nducement liability goes beyond that, and the distribution of the product can itself give rise to liability where evidence shows that the distributor intended and encouraged the product to be used to infringe." 545 U.S. at 940 n.13. Lower courts have similarly ruled that inducement must be active, and not merely based on encouragement. *See supra* § 4.11[6].

[5]*See Columbia Pictures Industries, Inc. v. Fung*, 710 F.3d 1020, 1032–33 (9th Cir. 2013); *supra* § 4.11[6][F].

[6]*See, e.g.*, *Columbia Pictures Industries, Inc. v. Fung*, 710 F.3d 1020

In *Global-Tech Appliances, Inc. v. SEB S.A.*,[7] a patent inducement case, the U.S. Supreme Court held that inducement liability may be premised on willful blindness, in addition to actual knowledge, but negligence or even recklessness would not suffice.[8] *SEB* is analyzed more extensively in section 8.10[3] and in connection with copyright inducement in section 4.11[6].

Unlike other grounds for imposing secondary copyright infringement, inducement necessarily involves a showing of bad intent. Because intent usually presupposes at least some level of knowledge, it is doubtful that a site or service that could be found liable for inducement could also benefit from the DMCA safe harbors.[9]

Where inducement is established, the *Sony* safe harbor likewise will not apply.[10]

Copyright inducement is analyzed more extensively in section 4.11[6].

49.05[3][F] Individual Liability of Owners and Investors

An owner of or investor in an Internet business found directly, contributorily or vicariously liable or liable for inducement, may face personal liability and be held vicariously liable if he or she had the right and ability to control the infringing conduct and had a direct financial interest in the activity of the entity held liable for infringement.[1] In addition, direct personal liability may be imposed for online acts of copyright infringement on corporate officers or site or service owners who personally participate in acts of

---

(9th Cir. 2013); *Arista Records LLC v. Lime Group LLC*, 784 F. Supp. 2d 398 (S.D.N.Y. 2011); *Arista Records LLC v. Usenet.com, Inc.*, 633 F. Supp. 2d 124 (S.D.N.Y. 2009); *see generally supra* § 4.11[6][F] (analyzing these and other inducement cases in greater detail).

[7]*Global-Tech Appliances, Inc. v. SEB S.A.*, 563 U.S. 754 (2011).

[8]*Global-Tech Appliances, Inc. v. SEB S.A.*, 563 U.S. 754, 765-66, 769-70 (2011).

[9]*See supra* §§ 4.11[6], 4.12[6][C].

[10]*See supra* § 4.11[6][B].

[Section 49.05[3][F]]

[1]*See, e.g., Playboy Enterprises, Inc. v. Webbworld, Inc.*, 991 F. Supp. 543, 554 (N.D. Tex. 1997), *aff'd mem.*, 168 F.3d 486 (5th Cir. 1999); *see generally supra* §§ 4.11, 49.05[4].

infringement.[2]

Where liability is based on inducement, an individual may be held jointly and severally liable with a business entity for his or her own acts of inducement. In *Columbia Pictures Industries, Inc. v. Fung*,[3] for example, the owner of various websites was named as a defendant and held individually liable for inducement. Similarly, in *Arista Records LLC v. Lime Group LLC*,[4] the court held Lime Wire, its parent company (Lime Group LLC) and its Chairman and sole Director (Mark Gorton) liable for copyright inducement under the 1976 Copyright Act and New York common law applicable to pre-1972 sound recordings.

Individual liability is analyzed in section 4.11[5][B].

49.05[3][G] Common Carrier Exemption

The Copyright Act contains an express exemption for passive carriers such as telephone companies that otherwise would be liable for secondary transmissions.[1] It is similar in principle to the exemption created for access providers under the CDA.[2] The common carrier exemption, however, has been held inapplicable to Internet access providers.[3]

---

[2]*See Playboy Enterprises, Inc. v. Russ Hardenburgh, Inc.*, 982 F. Supp. 503 (N.D. Ohio 1997) (holding a BBS owner jointly liable with the BBS itself).

[3]*Columbia Pictures Industries, Inc. v. Fung*, 710 F.3d 1020, 1031–39 (9th Cir. 2013); *supra* § 4.11[6].

[4]*Arista Records LLC v. Lime Group LLC*, 784 F. Supp. 2d 398 (S.D.N.Y. 2011).

[Section 49.05[3][G]]

[1]17 U.S.C.A. § 111.

[2]*See* 47 U.S.C.A. § 223(e)(1); *infra* § 54.03.

[3]*See Religious Technology Center v. Netcom On-Line Communication Services, Inc.*, 907 F. Supp. 1361, 1369 (N.D. Cal. 1995). The court rejected Netcom's argument that it was a common carrier that merely acted as a passive conduit for information because the statutory exemption is only available where a carrier does not have any direct or indirect control over the content or selection of the primary transmission. *See* 17 U.S.C.A. § 111(a)(3). The court wrote that it should be left to Congress to decide whether to create a new exemption for online service providers, although Judge Whyte acknowledged in *dicta* that

> [i]n a sense, a Usenet server that forwards all messages acts like a common carrier, passively retransmitting every message that gets sent through it. Netcom would seem no more liable than the phone company for carrying an infringing facsimile transmission or storing an infringing audio recording on its

49.05[3][H] Fair Use

Site owners and service providers may be able to rely upon the fair use defense in cases where unrelated third parties have used their services to post infringing material without their knowledge or assent. Fair use is a complete defense to copyright infringement, and applies where a work is used "for purposes such as criticism, comment, news reporting, teaching . . . scholarship or research . . . ."[1] In evaluating whether the fair use defense is available, courts must consider, in addition to other potentially relevant factors (such as the underlying constitutional objectives for copyright protection): (1) the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes; (2) the nature of the work; (3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and (4) the effect of the use upon the potential market for or value of the copyrighted work.[2]

Whether the fair use defense applies depends in part on who is asserting it. Thus, even where the person directly responsible would be held liable for copyright infringement, the owner of the site or service where the material was posted, stored or transmitted from, might to be able to successfully assert the fair use defense.[3] For example, in *Religious Technology Center v. Netcom On-Line Communication Services, Inc.*[4] the court found that an access provider had raised a factual dispute over its entitlement to assert the

---

voicemail . . . . [H]olding such a server liable would be like holding the owner of the highway, or at least the operator of a tollbooth, liable for the criminal activities that occur on its roads.

Religious Technology Center v. Netcom On-Line Communication Services, Inc., 907 F. Supp. 1361, 1369 n.12 (N.D. Cal. 1995).

The court instead analogized "Netcom's act of designing or implementing a system that automatically and uniformly creates temporary copies of all data sent through it" to the practice of allowing the public to use a photocopy machine. Judge Whyte wrote that, "[a]lthough some of the people using the machine may directly infringe copyrights, courts analyze the machine owner's liability under the rubric of contributory infringement, not direct infringement." *Id.* at 1369.

[Section 49.05[3][H]]

[1]17 U.S.C.A. § 107.

[2]17 U.S.C.A. § 107; *see supra* § 4.10.

[3]*See generally supra* § 4.10 (analyzing the fair use defense).

[4]*Religious Technology Center v. Netcom On-Line Communication*

defense in a case where the primary infringer was not entitled to assert it.[5] Similarly, use of a photo in connection with a blog post critical of the person shown in the picture, was held to be a fair use.[6]

While a site or service may be able to assert fair use for particular user files, fair use, unlike the DMCA, is rarely a defense on which a business model can be built. Fair use determinations are made based on a multipart balancing test and often turn on the unique facts of a given case. Predicting whether a use will be found fair is often limited by the fact that some details that could prove relevant in court may be unknowable (such as whether a given use *in fact* will adversely impact the market for the genuine product). Accordingly, any business model built around fair use almost by definition invites litigation.

Fair use is analyzed extensively in section 4.10[1].

49.05[3][I] The *Sony* Safe Harbor

As discussed above in connection with contributory infringement and vicarious liability, the Supreme Court has recognized a safe harbor in certain cases where liability is premised on a technology that has substantial non-infringing uses. The parameters of the *Sony* safe harbor are analyzed extensively in sections 4.10[5] and 4.11[6][B].

49.05[3][J] *De minimis* Doctrine

Under copyright law, *de minimis* acts of infringement are not actionable.[1] What constitutes *de minimis* copying is usu-

---

Services, Inc., 907 F. Supp. 1361 (N.D. Cal. 1995).

[5]*See Religious Technology Center v. Netcom On-Line Communication Services, Inc.*, 923 F. Supp. 1231, 1246 (N.D. Cal. 1995).

[6]*See Katz v. Google, Inc.*, 802 F.3d 1178 (11th Cir. 2015) (affirming the entry of summary judgment for the defendant-blogger in a suit where a real estate developer and part owner of the Miami Heat purchased the copyright to an unflattering image of himself and then sued the operator of a blog critical of his business practices for copyright infringement for displaying the image in connection with a critical post about him).

[Section 49.05[3][J]]

[1]E.g., *Tufenkian Import/Export Ventures, Inc. v. Einstein Moomjy, Inc.*, 338 F.3d 127, 131 (2d Cir. 2003) (holding that to prove infringement, a plaintiff must show "that the amount copied is more than *de minimis*"); *American Geophysical Union v. Texaco Inc.*, 60 F.3d 913, 916 (2d Cir. 1995); *Newton v. Diamond*, 388 F.3d 1189 (9th Cir. 2004) (affirming sum-

ally judged by the amount of a work that is copied.[2] In cyberspace, the *de minimis* doctrine should also be applied to the amount of *time* material remains online. Thus, a company that moves quickly to remove infringing material should not be held liable for infringement.[3]

49.06 Direct, Contributory, Vicarious and Inducing Trademark Infringement (and other liability under the Lanham Act)

Unlike copyright law, there is no Digital Millennium Trademark Act that provides a potential safe harbor for user generated content.[1] At the same time, the standards for imposing secondary trademark liability generally are tougher to meet than for secondary copyright infringement,[2] which reduces the potential risk of exposure for legitimate sites and services. In addition, in practice, many platforms respond to notices of alleged trademark infringement, and courts have been loath to impose liability on intermediaries based merely on generalized knowledge that a legitimate site or service could be used for infringement or in the absence of knowledge of specific alleged misconduct. Some site owners and service providers also may be able to benefit

---

mary judgment where the "use was *de minimis* and therefore not actionable."); *MiTek Holdings, Inc. v. ArcE Engineering Co.*, 89 F.3d 1548, 1559–60 (11th Cir. 1996); *CyberMedia, Inc. v. Symantec Corp.*, 19 F. Supp. 2d 1070, 1077 (N.D. Cal. 1998); *see generally supra* § 4.08[1].

[2]*See Sony Corp. of America v. Universal City Studios, Inc.*, 464 U.S. 417, 439 n.19 (1984) (characterizing the grounds on which contributory trademark infringement may be imposed as more narrowly drawn than for contributory copyright infringement); *see generally supra* §§ 49.05[3], 6.10[2].

[3]*See* Ian C. Ballon, *Pinning the Blame in Cyberspace: Towards A Coherent Theory for Imposing Vicarious Copyright, Trademark and Tort Liability for Conduct Occurring Over the Internet*, 18 Hastings J. Comm. & Ent. L. 733, 737–39 (1996).

[Section 49.06]

[1]*See supra* § 49.05.

[2]*See Sony Corp. of America v. Universal City Studios, Inc.*, 464 U.S. 417, 439 n.19 (1984); *see also AT&T Co. v. Winback & Conserve Program, Inc.*, 42 F.3d 1421, 1441 (3d Cir. 1994); *Perfect 10, Inc. v. Visa Int'l Service Ass'n*, 494 F.3d 788, 806 (9th Cir. 2007) ("The tests for secondary trademark infringement are even more difficult to satisfy than those required to find secondary copyright infringement."), *cert. denied*, 553 U.S. 1079 (2008); *Banff Ltd. v. Limited, Inc.*, 869 F. Supp. 1103, 1111 (S.D.N.Y. 1994). Third-party claims may not be based on dilution. *See supra* § 6.11[6].

from the innocent printer's and publisher's defense, which is analyzed more extensively in section 6.16[2][D] and discussed briefly later in this section. Potential limitations on a trademark owner's ability to enjoin service providers and internet publishers are discussed in section 6.16[1].

Although not an issue specific to platforms, when Lanham Act claims are premised on false designation or attribution, for material unprotected by copyright law (such as works in the public domain where the copyright has expired), or copying material potentially entitled to fair use, those claims may be preempted under the U.S Supreme Court's decision in *Dastar Corp. v. Twentieth Century Fox Film Corp.*,[3] which is analyzed extensively in section 6.12[1].

Because both damages and attorneys' fees under the Lanham Act generally are discretionary, rather than automatically recoverable by a prevailing plaintiff (other than in counterfeiting cases),[4] both trademark owners, on the one hand, and site owners and service providers, on the other, should theoretically have an incentive to work out any dispute, rather than risk litigation.

Some sites and services implement policies and procedures that mirror the DMCA.[5] Those that have adopted notice and takedown procedures, or which otherwise respond to rights owner complaints, and which terminate users who are infringers in appropriate circumstances, have been successful to date in avoiding liability, even in the absence of a statutory safe harbor such as the one created by the DMCA.[6] By contrast, those that turn a blind eye to user infringement risk significant exposure—particularly in counterfeiting cases or other instances where knowledge may be established or inferred and infringement is clearcut.

Internet intermediaries theoretically may be held liable for contributory trademark infringement or vicarious liability in narrow circumstances, if there is an underlying act of

---

[3]*Dastar Corp. v. Twentieth Century Fox Film Corp.*, 539 U.S. 23 (2003); *see generally supra* § 6.12.

[4]*See supra* § 6.16. In contrast to the general rule, damages in counterfeiting cases generally are recoverable, absent extenuating circumstances. *See supra* § 6.16[2][E].

[5]*See supra* § 49.05 (discussing the DMCA); *see generally supra* § 4.12 (analyzing the DMCA in greater detail).

[6]*See supra* § 49.05.

direct infringement by a user (or for their own misconduct).[7] The standards for proving trademark infringement are analyzed extensively in section 6.08. Unfair competition, false advertising and other related Lanham Act claims are addressed in section 6.12. Trademark dilution and claims under the Anticybersquatting Consumer Protection Act are analyzed in sections 6.11 and 7.06, respectively, although as set forth in those sections it is not clear that a claim for secondary infringement may be premised on either dilution or cybersquatting,[8] or that even if they could it would be possible to state a claim based on user generated content (although a site or service potentially could be held directly liable for its own misconduct under these laws). Lanham Act claims based on links, frames, metatags, sponsored links and banner advertisements are separately analyzed in chapter 9. Potential defenses, including fair use[9] and *de minimis* infringement,[10] are analyzed in chapter 6. If a defendant is not using a mark in a trademark sense, but is merely using it for noncommercial purposes, or if likelihood of confusion cannot be shown, or if fair use can be established, there will be no underlying act of infringement on which secondary liability could be imposed.

Contributory liability for trademark infringement may be established if a defendant: (1) intentionally induces another to infringe a trademark,[11] or (2) continues to supply a product knowing that the recipient is using it to engage in trademark infringement.[12] The Supreme Court's articulation of that test in *Inwood Laboratories, Inc. v. Ives Laboratories,*

---

[7]*See supra* § 6.10.

[8]*See supra* § 7.14.

[9]*See supra* § 6.14.

[10]*See supra* § 6.15.

[11]In *Global-Tech Appliances, Inc. v. SEB S.A.*, 563 U.S. 754 (2011), a patent inducement case, the U.S. Supreme Court held that inducement liability may be premised on willful blindness, in addition to actual knowledge, but that negligence or even recklessness would not suffice. *See id.* at 765-66, 269-70. This case will likely be viewed as persuasive authority in future trademark inducement cases.

SEB is analyzed more extensively in section 8.10[3] and in connection with potential claims for inducing trademark infringement in section 6.10[1].

[12]*See, e.g.*, *Inwood Laboratories, Inc. v. Ives Laboratories, Inc.*, 456 U.S. 844, 854–55 (1982) (pharmaceutical manufacturer-distributor that supplied generic drugs in such a way that induced some pharmacists to mislabel the products as brand name drugs); *Polymer Technology Corp. v.*

Inc.,[13] focused on *manufacturers, distributors* and *products.*[14] When an alleged direct infringer supplies a service rather than a product, under the second prong of this test, courts in the Ninth Circuit and elsewhere first require consideration of the extent of control exercised by the defendant over the third-party's means of infringement.[15] For liability potentially

---

Mimran, 975 F.2d 58, 64 (2d Cir. 1992) (remanding for further consideration a case involving the sale of professional kit contact lenses where it "would not have taken a great leap of imagination" to realize that the purchaser could not resell the kits without repackaging them); *Coach, Inc. v. Goodfellow*, 717 F.3d 498, 503–05 (6th Cir. 2013) (affirming judgment for contributory liability against a flea market operator who continued to rent booths and storage units to vendors who he knew or had reason to know were selling counterfeit Coach products based on his receipt of notices from Coach and knowledge of police raids); *Hard Rock Cafe Licensing Corp. v. Concession Services, Inc.*, 955 F.2d 1143, 1149 (7th Cir. 1992) (flea market operator); *Fonovisa, Inc. v. Cherry Auction, Inc.*, 76 F.3d 259 (9th Cir. 1996) (flea market operator); *Procter & Gamble Co. v. Haugen*, 317 F.3d 1121, 1128–29 (10th Cir. 2003) (following *Inwood* and Ninth Circuit case law in holding that Amway could not be held contributorily liable for the conduct of its distributors); *Mini Maid Services Co. v. Maid Brigade Systems, Inc.*, 967 F.2d 1516, 1521–22 (11th Cir. 1992) (extending the doctrine to a franchisor/franchisee relationship but holding that the district court erred in finding contributory liability based on the franchisor's failure to supervise the franchisee with reasonable diligence); *A & M Records, Inc. v. Abdallah*, 948 F. Supp. 1449 (C.D. Cal. 1996) (holding contributorily liable a defendant who continued to supply blank, "time-loaded" audio cassettes to his customers, even though he knew that those cassettes were used to engage in trademark infringement); *Polo Ralph Lauren Corp. v. Chinatown Gift Shop*, 855 F. Supp. 648 (S.D.N.Y. 1994) (holding that plaintiff stated a claim for contributory infringement by alleging that landlords knowingly failed to prevent tenants' sale of counterfeit goods).

[13]*Inwood Laboratories, Inc. v. Ives Laboratories, Inc.*, 456 U.S. 844 (1982).

[14]The Court specifically held that liability could be imposed "if 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 . . . ." *Inwood Laboratories, Inc. v. Ives Laboratories, Inc.*, 456 U.S. 844, 854 (1982).

[15]*See Louis Vuitton Malletier, S.A. v. Akanoc Solutions, Inc.*, 658 F.3d 936 (9th Cir. 2011); *Perfect 10, Inc. v. Visa Int'l Service Ass'n*, 494 F.3d 788, 807 (9th Cir. 2007) (affirming dismissal of a claim brought against payment processing services that allowed infringing websites to accept credit card payments), *cert. denied*, 553 U.S. 1079 (2008); *Lockheed Martin Corp. v. Network Solutions, Inc.*, 194 F.3d 980, 984 (9th Cir. 1999) (holding that a domain name registrar could not be held liable merely for registering names that were subsequently used to engage in infringement); *Tiffany*

to attach under this standard, there must be "direct control and monitoring of the instrumentality used by a third party to infringe plaintiff's mark."[16] Where direct control and monitoring exists, the elements of the traditional test must then be satisfied to establish liability.

A determination of contributory infringement depends upon a defendant's intent (for inducement) and its knowledge of the wrongful activities.[17] Where knowledge exists, the doctrine prevents a third party from disregarding "blatant trademark infringements with impunity."[18] The knowledge required to establish liability in Internet cases based on continuing to supply a product or service must be *specific* or *particularized.* Generalized knowledge that a site or service could be used for infringement is not enough under

---

(NJ) Inc. v. eBay, Inc., 576 F. Supp. 2d 463 (S.D.N.Y. 2008) (holding that where liability is premised on the conduct of a user of a venue, an initial threshold showing—direct control and monitoring over the means of infringement—must be made), *aff'd,* 600 F.3d 93 (2d Cir.) (assuming that this test applied without deciding whether it was in fact appropriate), *cert. denied,* 562 U.S. 1082 (2010).

[16]*Perfect 10, Inc. v. Visa Int'l Service Ass'n*, 494 F.3d 788, 807 (9th Cir. 2007), *cert. denied*, 553 U.S. 1079 (2008); *Lockheed Martin Corp. v. Network Solutions, Inc.*, 194 F.3d 980, 984 (9th Cir. 1999); *Stayart v. Yahoo! Inc.*, 651 F. Supp. 2d 873 (E.D. Wis. 2009) (dismissing plaintiff's claim for contributory infringement; "Even after receiving Stayart's complaints, Yahoo! cannot be held liable for failing to remove the offending search results. Yahoo! did not create the offending content and did not exert any control over the third-party websites where the alleged infringement occurred."), *aff'd on other grounds,* 623 F.3d 436 (7th Cir. 2010) (holding that plaintiff did not have standing to bring a Lanham Act claim based on use of her name); *SB Designs v. Reebok Int'l, Ltd.*, 338 F. Supp. 2d 904, 913–14 (N.D. Ill. 2004) (applying Lockheed Martin in holding that a defendant that exerted no control over an allegedly infringing third-party website cannot be held contributorily liable). *But see Medline Industries, Inc. v. Strategic Commercial Solutions, Inc.*, 553 F. Supp. 2d 979, 992 n.3 (N.D. Ill. 2008) (disagreeing with the *SB Designs* court that the Seventh Circuit has adopted the Ninth Circuit's requirement that a plaintiff must plead that the defendant directly controlled and monitored the instrumentality of infringement used by the direct infringer and declining to impose that requirement in denying the defendant's motion to dismiss).

[17]*See David Berg & Co. v. Gatto Int'l Trading Co.*, 884 F.2d 306, 311 (7th Cir. 1989). An express finding of intent, however, is not required. *See Louis Vuitton Malletier, S.A. v. Akanoc Solutions, Inc.*, 658 F.3d 936 (9th Cir. 2011); *see generally supra* § 6.10[1].

[18]*Fonovisa, Inc. v. Cherry Auction, Inc.*, 76 F.3d 259, 265 (9th Cir. 1996) (imposing liability on a swap meet owner).

current case law.[19] In other words, liability may not be imposed based merely on the foreseeability that a site or service could be used improperly in violation of user rules or contractual obligations. In addition, while "willful blindness is inexcusable under contributory infringement law,"[20] it does not "impose . . . an affirmative duty to seek out potentially infringing uses" by third parties.[21]

Merely sending a site or service a letter alleging infringement may not be sufficient to establish knowledge.[22] On the

---

[19]*See, e.g., Tiffany (NJ) Inc. v. eBay Inc.*, 600 F.3d 93, 107–09 (2d Cir.), *cert. denied*, 562 U.S. 1082 (2010); *Rosetta Stone Ltd. v. Google, Inc.*, 676 F.3d 144, 163 (4th Cir. 2012); *1-800-Contacts, Inc. v. Lens.com, Inc.*, 722 F.3d 1229, 1253 (10th Cir. 2013); *Ohio State University v. Teespring, Inc.*, Case No. 2:14-cv-397, 2015 WL 13016358, at *4-5 (S.D. Ohio Apr. 13, 2015) (dismissing plaintiff's claim for contributory trademark infringement where OSU could not plausibly allege more than general knowledge that people might use Teespring's online T-shirt printing service to engage in infringement); *Sellify Inc. v. Amazon.com, Inc.*, No. 09 Civ. 0268 (JSR), 2010 WL 4455830, at *4 (S.D.N.Y. Nov. 14, 2010) (granting summary judgment for Amazon.com on the issue of contributory infringement where there was "no evidence that Amazon had particularized knowledge of, or direct control over," third-party sponsored link advertisements purchased by an Amazon.com associate to generate sales); *see also Academy of Motion Picture Arts & Sciences v. GoDaddy.com, Inc.*, Case Nos. CV 10-03738 AB (CWx), CV 13-08458 (CW), 2015 WL 5311085, at *35 (C.D. Cal. Sept. 10, 2015) (holding that generalized knowledge is likewise an insufficient basis for imposing liability under the Anti-Cybersquatting Consumer Protection Act). *But see 1-800-Contacts, Inc. v. Lens.com, Inc.*, 722 F.3d 1229, 1252-54 (10th Cir. 2013) (holding that the requirement that knowledge be specific and particularized with respect to an alleged act of infringement does not mean that a defendant has no duty to act unless and until it obtains that knowledge for a specific individual offender); *see generally supra* § 6.10[1].

[20]*Ford Motor Co. v. Greatdomains.com, Inc.*, 177 F. Supp. 2d 635, 646 (E.D. Mich. 2001) (holding a domain name auction site not contributorily liable), *citing Hard Rock Cafe Licensing Corp. v. Concession Services, Inc.*, 955 F.2d 1143, 1149 (7th Cir. 1992).

[21]*Lockheed Martin Corp. v. Network Solutions, Inc.*, 985 F. Supp. 949, 951 (C.D. Cal. 1997) (referring to the obligations of a registrar in accepting domain name registrations), *aff'd on other grounds*, 194 F.3d 980 (9th Cir. 1999); *see also Hard Rock Cafe Licensing Corp. v. Concession Services, Inc.*, 955 F.2d 1143, 1149 (7th Cir. 1992) (finding no duty on the part of a flea market owner to take precautions against potential acts of infringement by vendors).

[22]*See, e.g., Tiffany (NJ) Inc. v. eBay, Inc.*, 576 F. Supp. 2d 463, 511 (S.D.N.Y. 2008) ("mere assertions and demand letters are insufficient to impute knowledge as to instances not specifically identified in such notices, particularly in cases where the activity at issue is not always infringing."),

other hand, even if a site or service is not necessarily required to remove content or suspend or terminate a user every time a mere allegation of infringement is made, failing to respond to a communication could lead to liability, depending on the facts of a given case. For example, Internet intermediaries and their individual owners may be held liable for contributory infringement where they ignore multiple complaints (or where the same counterfeiters reappear at new locations hosted by the same service after being taken down in response to a notice from the mark owner).[23] In *Louis Vuitton Malletier, S.A. v. Akanoc Solutions, Inc.*,[24] where at least 18 infringement notices went unanswered, a jury in San Jose, California in 2009 awarded luxury goods manufacturer Louis Vuitton $31,500,000 in statutory damages for contributory trademark infringement against three defendants (which was subsequently reduced in a post-trial ruling and on appeal to joint and several liability of $10,500,000 against two of the defendants). *Akanoc* underscores the risk of exposure faced by sites and services that do not adequately respond to notices from rights owners or turn a blind eye to counterfeiting or other obvious infringement.

Sites and services therefore would be well advised to respond to trademark-related complaints, rather than simply

---

aff'd, 600 F.3d 93, 109 & n.13 (2d Cir.), *cert. denied*, 562 U.S. 1082 (2010); *Fare Deals Ltd. v. WorldChoiceTravel.com, Inc.*, 180 F. Supp. 2d 678, 690–91 (D. Md. 2001) (finding insufficient a demand letter notifying the defendant of plaintiff's position); *Gucci America, Inc. v. Hall & Associates*, 135 F. Supp. 2d 409, 420 (S.D.N.Y. 2001) (holding that a "trademark owner's mere assertion that its domain name is infringed is insufficient to impute knowledge of infringement," and a demand letter is also insufficient); *Lockheed Martin Corp. v. Network Solutions, Inc.*, 985 F. Supp. 949, 964 (C.D. Cal. 1997) (holding that a "trademark owner's demand letter is insufficient to resolve . . . uncertainty" of infringement), *aff'd*, 194 F.3d 980 (9th Cir. 1999); *Coca-Cola Co. v. Snow Crest Beverages*, 64 F. Supp. 980, 987 (D. Mass. 1946) (holding, in a case cited by the *U.S. Supreme Court in Inwood Laboratories, Inc. v. Ives Laboratories, Inc.*, 456 U.S. 844 (1982) that generalized complaints about counterfeiting is insufficient to establish knowledge); *see generally supra* § 6.10[1] (analyzing the difference between notice and knowledge in greater detail).

[23]*See Louis Vuitton Malletier, S.A. v. Akanoc Solutions, Inc.*, 591 F. Supp. 2d 1098, 1112–13 (N.D. Cal. 2008) (denying summary judgment and finding a triable issue on these facts).

[24]*Louis Vuitton Malletier, S.A. v. Akanoc Solutions, Inc.*, No. C 07-03952 JW, 2009 WL 3062893 (N.D. Cal. Aug. 28, 2009), *aff'd in part, rev'd in part,* 658 F.3d 936 (9th Cir. 2011); *see generally supra* § 6.10[2][A] (analyzing the case in greater detail).

ignoring them.

Internet businesses that have adopted policies of first warning and then terminating users who engage in infringing conduct also have been able to argue effectively that contributory liability should not be imposed because they have not "continued to supply" an infringing service within the meaning of *Inwood* after arguably acquiring knowledge of infringement.[25] Where a complaint involves counterfeiting or other clear violations, a site or service may choose to terminate a user immediately, whereas a warning may be sufficient where it will likely lead to the user discontinuing allegedly infringing conduct (or where a mere allegation of infringement does not identify content or conduct that in fact appears to be infringing). Regardless of whether a user is warned or terminated, infringing or counterfeit material should be removed immediately when it is clearly identified as such, assuming that it is hosted by the site or service (or that the intermediary is otherwise able to remove it).[26]

---

[25]*See Tiffany (NJ) Inc. v. eBay Inc.*, 600 F.3d 93 (2d Cir.) (affirming judgment for eBay on Tiffany's claim for contributory infringement), *cert. denied,* 562 U.S. 1082 (2010); *Sellify Inc. v. Amazon.com, Inc.,* No. 09 Civ. 0268 (JSR), 2010 WL 4455830 (S.D.N.Y. Nov. 14, 2010) (granting summary judgment for Amazon.com); *see generally supra* §§ 6.10[2][A], 6.10[2][I], 6.10[2][J] (discussing these cases in greater detail).

[26]Both eBay, in *Tiffany (NJ) Inc. v. eBay Inc.*, 600 F.3d 93 (2d Cir.), *cert. denied,* 562 U.S. 1082 (2010), and Amazon.com, in *Sellify Inc. v. Amazon.com, Inc.,* No. 09 Civ. 0268 (JSR), 2010 WL 4455830 (S.D.N.Y. Nov. 14, 2010), had adopted policies of terminating repeat infringers that were cited approvingly by the courts in their respective cases. In *Tiffany v. eBay*, eBay had removed every listing identified in response to notices sent by Tiffany—including some that later turned out to have involved genuine products. In *Sellify*, Amazon.com had not removed the advertisement at issue because it could not do so. An Amazon.com associate (not Amazon.com) had placed the advertisement with Google. Amazon.com sent a warning notice in response to the first letter it received from the plaintiff and terminated the user's account (and stopped payments to it) upon learning from the second notice that the allegedly infringing advertisements had not been discontinued.

Where a site or service actually hosts the allegedly infringing material, it may face a higher burden to actually remove the material, depending on the facts of the case. In *Louis Vuitton Malletier, S.A. v. Akanoc Solutions, Inc.*, 658 F.3d 936 (9th Cir. 2011), for example, liability was imposed in a counterfeiting case where the defendant did not do so.

Akanoc also illustrates that it may be easier for a mark owner to establish liability in cases involving counterfeiting than in disputes where user infringement is less clear-cut or that raise fair use issues or other potential defenses. Greater vigilance may be required from site owners

While platforms that host user content may have some risk of exposure for contributory infringement, vicarious trademark liability could not be imposed on a legitimate site or service merely because of user misconduct or the presence of unauthorized infringing material posted, transmitted or stored by a user. To establish vicarious liability, a defendant and the direct infringer must have "an apparent or actual partnership, have authority to bind one another in transactions with third parties, or exercise joint ownership or control over the infringing product."[27] The doctrine has not been universally adopted, and therefore may not necessarily be applied in all circuits.[28] Where it is recognized, vicarious liability must be based on agency law principles, rather than the broader concepts of vicarious liability applicable under tort or copyright law.[29] Although based in principle on agency principles, vicarious trademark liability may be imposed

---

and service providers in cases involving counterfeiting or obvious infringement.

More broadly, these cases reflect that companies that adopt compliance-oriented policies to deter infringement are less likely to be held secondarily liable for the conduct of their users than those that do not.

[27]*See, e.g., Fonovisa, Inc. v. Cherry Auction, Inc.*, 847 F. Supp. 1492, 1498 (E.D. Cal. 1994), *rev'd on other grounds,* 76 F.3d 259, 263 (9th Cir. 1996); *see also David Berg & Co. v. Gatto Int'l Trading Co.*, 884 F.2d 306, 311 (7th Cir. 1989); *Gucci America, Inc. v. Frontline Processing Corp.*, 721 F. Supp. 2d 228 (S.D.N.Y. 2010) (articulating this standard in holding that the plaintiff had failed to state a claim, while also noting that the Second Circuit has not actually applied the doctrine); *Stayart v. Yahoo! Inc.*, 651 F. Supp. 2d 873 (E.D. Wis. 2009) (dismissing plaintiff's claim for vicarious liability arising out of Yahoo!'s alleged failure to remove offending search results from a third-party website that it did not create and had no control over; "Yahoo! cannot be vicariously liable without 'a finding that the defendant and the infringer have an apparent or actual partnership, have authority to bind one another in transactions with third parties or exercise joint ownership or control over the infringing product.' "), *aff'd on other grounds,* 623 F.3d 436 (7th Cir. 2010); *Banff Ltd. v. Limited, Inc.*, 869 F. Supp. 1103, 1111 (S.D.N.Y. 1994) (quoting the lower court decision in *Fonovisa* without adopting the standard).

[28]*800-JR Cigar, Inc. v. GoTo.com, Inc.*, 437 F. Supp. 2d 273, 281 (D.N.J. 2006) (stating in *dicta* that the Third Circuit has declined to adopt the doctrine of vicarious trademark infringement), *citing AT&T Co. v. Winback & Conserve Program, Inc.*, 42 F.3d 1421, 1431 (3d Cir. 1994); *Banff Ltd. v. Limited, Inc.*, 869 F. Supp. 1103, 1111 (S.D.N.Y. 1994) (discussing other cases); *supra* § 6.10 (analyzing the issue).

[29]*See AT&T Co. v. Winback & Conserve Program, Inc.*, 42 F.3d 1421, 1434 (3d Cir. 1994); *see also Symantec Corp. v. CD Micro, Inc.*, 286 F. Supp. 2d 1265, 1275 (D. Or. 2003) (declining to impose vicarious liability

even where the party directly liable is an independent contractor.[30]

Unlike the Copyright Act—which imposes strict liability where a defendant copies a protected work—under trademark law, infringement may not be established merely because a defendant reproduced a mark. To prevail, a plaintiff must show, among other things, likelihood of confusion or dilution (based on tarnishment of blurring).[31] Trademark rights may be strong or weak, depending on the strength of the mark, and broad or narrow, depending on third-party uses of the same or similar marks.[32] In addition, to establish secondary infringement, knowledge (either actual or imputed), intent or active participation must be shown, which can be more difficult where the direct infringer is unknown. Unlike under copyright law, vicarious liability may not be established merely by a showing of a direct financial interest and a right and ability to control.[33]

Indirect trademark liability has been imposed on manufacturers and others involved in the distribution of infringing products[34] and on landlords or operators of flea markets.[35] Given the narrow scope of potential liability, however, secondary liability typically has not been imposed on Internet or mobile platforms absent inducement or specific knowledge of ongoing acts of infringement and a deliberate choice to ignore that information. Merely operating a legitimate site or service where users engage in isolated acts of misconduct should not be enough to impose liability.

While some courts have ruled that plaintiffs could state

---

for trademark infringement on the CEO of a company held liable for selling pirated software over the Internet who was held vicariously liable for copyright infringement because he had the right and ability to control the acts of the corporation, based on the court's conclusion without substantial analysis that the scope of liability for vicarious trademark infringement was narrower than for vicarious copyright infringement).

[30]*See AT&T Co. v. Winback & Conserve Program, Inc.*, 42 F.3d 1421, 1434 (3d Cir. 1994).

[31]*See supra* §§ 6.08, 6.11.

[32]*See supra* §§ 6.02[2], 6.08.

[33]*See supra* § 4.11.

[34]E.g., *Inwood Laboratories, Inc. v. Ives Laboratories, Inc.*, 456 U.S. 844, 854–55 (1982).

[35]*See Hard Rock Cafe Licensing Corp. v. Concession Services, Inc.*, 955 F.2d 1143, 1149 (7th Cir. 1992); *Fonovisa, Inc. v. Cherry Auction, Inc.*, 76 F.3d 259, 264 (9th Cir. 1996).

claims for secondary liability in cases over user content brought against Internet sites and services,[36] none of these cases involved blog posts or material on social network profiles. Indeed, because a Lanham Act claim requires a showing that a defendant's use be undertaken in connection with the sale of goods or services or substantial advertising,[37] it could be difficult for a mark owner to establish liability on the part of a site or service when the underlying act may be noncommercial and therefore not actionable.[38] Of course, where user generated content is offered in connection with the sale of goods or services or substantial advertising, it potentially could be actionable (and banner ads, which are ubiquitous on blogs and other sites, could qualify as substantial advertising, although in many cases it would be the site, not the user, that was generating the ad revenue, which would not change the nature of the underlying use if that use was noncommercial).[39]

Louis Vuitton Malletier, S.A. v. Akanoc Solutions, Inc.[40] involved counterfeit goods websites that were hosted by

---

[36]*See, e.g., Vulcan Golf, LLC v. Google Inc.*, 552 F. Supp. 2d 752, 770 (N.D. Ill. 2008) (ruling that the plaintiff had stated a claim for contributory infringement against Google, Inc. by alleging that it was aware of the allegedly infringing nature of the domain names that it advertised); *GEICO v. Google, Inc.*, 330 F. Supp. 2d 700, 704–05 (E.D. Va. 2004) (denying defendants Google, Inc., and Overture Services, Inc.'s motions to dismiss federal Lanham Act claims for trademark infringement, contributory trademark infringement, vicarious trademark infringement, false representation and dilution arising out of their practice of selling advertisements linked to search terms); *see also Perfect 10, Inc. v. Cybernet Ventures, Inc.*, 167 F. Supp. 2d 1114, 1122 (C.D. Cal. 2001) (holding that the operator of a website that provided gateway and quality assurance services to adult websites could be held directly liable for trademark violations by its customers if a partnership relationship was found to exist between the operator and its customers).

In *GEICO*, Judge Leonie Brinkema of the Eastern District of Virginia held that plaintiff stated a claim for contributory infringement by alleging that Google encouraged advertisers to bid on trademarked words and monitored and controlled the allegedly infringing third-party advertisements. 330 F. Supp. 2d at 705. She likewise ruled that GEICO stated a claim for vicarious liability by alleging that both Overture and its advertisers controlled the appearance of the advertisements on Overture's search results page, including the use of GEICO trademarks on that page. Liability for sponsored links is separately addressed in section 9.11.

[37]*See supra* § 7.10.

[38]*See supra* § 6.14.

[39]*See supra* § 6.14[5].

[40]*Louis Vuitton Malletier, S.A. v. Akanoc Solutions, Inc.*, 658 F.3d 936

defendants—not typical user generated content—although a blog operator or other site owner or service provider potentially could be held liable for user misconduct on their sites where they fail to respond adequately.

Payment processors also potentially could be held contributorily liable, in narrow circumstances, for providing services to websites that traffic in counterfeit goods,[41] although not in the Ninth Circuit.[42]

In addition to contributory liability, sites and services potentially may be held directly liable for their own misconduct (if any), which, if applicable, requires a lower showing of proof than secondary liability. In older cases, bulletin board services and some ISPs had been held directly liable for operating services that included material uploaded by users.[43]

Some courts also recognize "joint tortfeasor" liability. Although vicarious liability will not be found where there is no agency or equivalent relationship between the site or service and the direct infringer,[44] "joint tortfeasor" liability, where it is recognized, may be imposed by some courts on more remotely involved defendants or the owners or operators of entities held liable, based on tort theories of joint liability or conspiracy.[45]

(9th Cir. 2011).

[41]*See Gucci America, Inc. v. Frontline Processing Corp.*, 721 F. Supp. 2d 228 (S.D.N.Y. 2010).

[42]*See Perfect 10, Inc. v. Visa Int'l Service Ass'n*, 494 F.3d 788 (9th Cir. 2007), *cert. denied*, 553 U.S. 1079 (2008). The court in *Gucci*, which was cited in the preceding footnote, followed Chief Judge Kozinski's dissenting opinion in *Visa*.

[43]*See supra* § 6.10[2] (discussing cases).

[44]*See, e.g., Sellify Inc. v. Amazon.com, Inc.,* No. 09 Civ. 0268 (JSR), 2010 WL 4455830, at *2–3 (S.D.N.Y. Nov. 14, 2010) (granting summary judgment for Amazon.com on plaintiff's claim for vicarious trademark infringement over third-party sponsored link advertisements purchased by one of Amazon.com's more than 3 million associates, where there was no agency relationship or actual or apparent authority); *Fare Deals Ltd. v. WorldChoiceTravel.com, Inc.*, 180 F. Supp. 2d 678, 684–86 (D. Md. 2001) (dismissing plaintiff's claim for vicarious liability against the operators of the Faredeals.com travel website based on the conduct of one of its affiliates where the affiliate agreement provided that the parties were independent contractors and the degree of control exercised was minimal).

[45]*See, e.g., TrafficSchool.com, Inc. v. eDriver, Inc.*, 633 F. Supp. 2d 1063, 1082 (C.D. Cal. 2008) (citing other cases), *aff'd in relevant part,* 653

In *Tiffany (NJ) Inc. v. eBay, Inc.*,[46] the Second Circuit affirmed the entry of judgment for eBay following a bench trial based on the finding that it could not be held contributorily liable where it had only generalized knowledge that its site could be used to sell unauthorized products (in addition to legitimate products) and where it promptly discontinued listings in every single instances where it was given specific notice by Tiffany's and terminated the access rights of repeat infringers. The court in *Tiffany v. eBay* also made clear that secondary liability, not direct infringement, is the operative theory in a suit brought against a platform, based on user content or conduct.[47]

The Second Circuit's decision in *Tiffany (NJ) Inc. v. eBay, Inc.*, and *Louis Vuitton Malletier, S.A. v. Akanoc Solutions, Inc.*,[48] in which the Ninth Circuit largely affirmed a jury verdict of contributory trademark infringement in a case

---

F.3d 820 (9th Cir. 2011).

[46]*Tiffany (NJ) Inc. v. eBay Inc.*, 600 F.3d 93 (2d Cir.), *cert. denied*, 562 U.S. 1082 (2010); *see generally supra* § 6.10[2][I] (analyzing the case in greater detail).

[47]*See, e.g.*, *Tiffany (NJ) Inc. v. eBay, Inc.*, 600 F.3d 93, 103 (2d Cir.) ("eBay's knowledge *vel non* that counterfeit Tiffany wares were offered through its website is relevant to the issue of whether eBay contributed to the direct infringement of Tiffany's mark by the counterfeiting vendors themselves, or whether eBay bears liability for false advertising. But it is not a basis for a claim of direct trademark infringement against eBay . . . ."), *cert. denied*, 562 U.S. 1082 (2010); *Lasoff v. Amazon.com Inc.*, Case No. C-151 BJR, 2017 WL 372948, at *7-8 (W.D. Wash. Jan. 26, 2017) (applying *Tiffany v. eBay* in granting summary judgment for Amazon.com on plaintiff's claim for direct trademark infringement in a case arising out of Amazon.com's alleged use of his mark in sponsored links advertisements, in addition to granting summary judgment for Amazon.com on plaintiff's state law claims under the CDA); *Altinex v. Alibaba.com Hong Kong Ltd.*, SACV 13-01545 JVS (RNBx), 2016 WL 6822235, at *4-7 (C.D. Cal. Mar. 25, 2016) (granting summary judgment for Alibaba on plaintiff's claim for direct trademark infringement arising out of user listings where the evidence showed that Alibaba removed the listings after receiving notice and there was no evidence to support plaintiff's allegation that the platform had designed its search tool to facilitate user access to counterfeit versions of plaintiff's products); *Perfect 10, Inc. v. Giganews, Inc.*, CV11-07098 AHM (SHx), 2013 WL 2109963 (C.D. Cal. Mar. 8, 2013) (holding that plaintiff had failed to state a claim for direct trademark against defendants for "providing access to a forum where content bearing a trademark may be obtained" from third parties; "Direct infringement requires that the defendant itself 'use' the mark; it is insufficient for direct infringement purposes to allege that a defendant allows third parties to use the mark.").

[48]*Louis Vuitton Malletier, S.A. v. Akanoc Solutions, Inc.*, 658 F.3d 936

where a web host ignored 18 notices of infringement, underscore two important practical points for site owners and service providers. First, the safer approach for Internet sites and services is to simply remove a listing in response to a specific notice, even if case law suggests that merely receiving a notice may not necessarily mean that a site or service has knowledge of infringement. Second, platforms that implement extensive antipiracy protections and do more than the law requires, such as eBay, are less likely to be held liable. By contrast, intermediaries such as the web hosts at issue in *Akanoc* that do not reply to takedown notices and generally turn a blind eye to infringement are more likely to be found liable for the misdeeds of their customers or users.[49]

One district court, in a case involving *SunFrog.com*, suggested in *dicta* that *Tiffany v. eBay* shouldn't apply to the offline activities of a print-on-demand business,[50] but there is no basis to draw this distinction and at least one other court had reached a contrary conclusion.[51]

The unique facts of *SunFrog* also may make it distinguishable from other cases involving print-on-demand services. In *SunFrog,* the court found that during the relevant time period, when it was just getting started, the company was slow to respond to numerous notices and engaged in willful blindness.[52] It also was "deeply and indispensably involved in the creation of its design listings, including offering the software to make them, holding prior designs for later use in the All Art database, and aggressively advertising those list-

---

(9th Cir. 2011); *see generally supra* § 6.10[2][A].

[49]A rights owner who receives no response to a takedown notice is more likely to get frustrated and assume that a site or service is not compliance-oriented—and ultimately may be more likely to file suit. This may be true even where a site or service in fact removes some material, but omits to notify the rights owner who may assume the site took no action.

[50]*See H-D U.S.A., LLC v. SunFrog, LLC*, 311 F. Supp. 3d 1000 (E.D. Wisc. 2018).

[51]*See Ohio State University v. Teespring, Inc.*, Case No. 2:14-cv-397, 2015 WL 13016358, at *4-5 (S.D. Ohio Apr. 13, 2015) (dismissing plaintiff's claim for contributory trademark infringement where OSU could not plausibly allege more than general knowledge that people might use Teespring's online T-shirt printing service to engage in infringement).

[52]*See H-D U.S.A., LLC v. SunFrog, LLC*, 311 F. Supp. 3d 1000, 1038-39 (E.D. Wisc. 2018), *appeal dismissed*, Appeal No. 18-2073, 2018 WL 6039900 (7th Cir. July 19, 2018).

ings through Facebook and other social media."[53] The court declined to decide whether an "entirely automated and user-directed" service could be liable for merely providing back end printing services to users.[54]

In general, platforms, sites and services that seek to deter infringement will be cut more slack by judges and juries when they make mistakes than those that do the bare minimum or less, which have a higher practical risk of liability (and, like the defendants in *Akanoc*, may be held liable for substantial damages).

Some Internet sites and services, including blogs, may be able to qualify for the innocent printer's and publishers defense discussed in section 6.16[2][D]. A monetary award may not be granted—and only injunctive relief against future printing or publishing may issue—against (1) printers ("[w]here an infringer or violator is engaged solely in the business of printing the mark or violating matter for others") and (2) publishers or distributors of newspapers, magazines, other similar periodicals or electronic communications where the infringement or violation complained of is contained in or is part of a paid advertisement in the periodical or "electronic communication."[55] The showings required for a defendant to qualify for this defense (innocence and lack of knowledge)[56] and a plaintiff to prove secondary liability ultimately are mutually exclusive. While an "innocent" party that acted reasonably may be able to avoid liability, the defense is unlikely to apply to an intermediary with knowledge of the infringement (and even more clearly would not apply to one found liable for inducement or willful blindness). If a site owner or service provider may be eligible for the innocent printer defense, it should adopt practices and procedures to deter infringing use of its site and ensure that notices of infringement are promptly addressed.

---

[53]*See H-D U.S.A., LLC v. SunFrog, LLC*, 311 F. Supp. 3d 1000, 1038 (E.D. Wisc. 2018), *appeal dismissed*, Appeal No. 18-2073, 2018 WL 6039900 (7th Cir. July 19, 2018).

[54]*See H-D U.S.A., LLC v. SunFrog, LLC*, 311 F. Supp. 3d 1000, 1037 (E.D. Wisc. 2018), *appeal dismissed*, Appeal No. 18-2073, 2018 WL 6039900 (7th Cir. July 19, 2018).

[55]15 U.S.C.A. § 1114(2); *see also Hendrickson v. eBay, Inc.*, 165 F. Supp. 2d 1082 (C.D. Cal. 2001) (holding eBay entitled to the defense); *see generally supra* § 6.16[2][D].

[56]*See supra* § 6.16[2][D] (analyzing the defense and its required elements in greater detail).

When injunctive relief is sought against an internet printer or publisher, the Ninth Circuit has held, in an analogous context under the Copyright Act, that an injunction compelling a service provider to remove user content is deemed to be a mandatory injunction, which is disfavored.[57] It may also be viewed as an impermissible prior restraint.[58]

The risk of secondary liability for individual corporate officers for the infringing activities of their companies is separately analyzed in section 6.10[4].

The Ninth Circuit has held that secondary liability doctrines may not extend to claims under the Anticybersquatting Consumer Protection Act.[59]

A small number of district courts have entertained claims for contributory dilution,[60] but it is questionable whether Congress intended to allow for secondary liability when it enacted the Federal Trademark Dilution Act in 1996 or the Trademark Dilution Revision Act of 2006 (and the same rationale for finding no implied claim for secondary liability under the ACPA in 15 U.S.C.A. § 1125(d) applies as well to dilution claims under section 1125(c)).[61]

The Second[62] and Eleventh[63] Circuits have recognized a potential cause of action for contributory false advertising,

---

[57]*Garcia v. Google, Inc.*, 786 F.3d 733, 740 & n.4 (9th Cir. 2015) (*en banc*); *supra* §§ 4.13[1] (discussing the case), 6.16[1] (analyzing injunctive relief under the Lanham Act).

[58]*See Garcia v. Google, Inc.*, 786 F.3d 733, 746-47 (9th Cir. 2015) (*en banc*) (dissolving a previously entered preliminary injunction compelling YouTube to take down copies of the film "Innocence of Muslims" and take all reasonable steps to prevent further uploads, which the *en banc* panel held had operated as a prior restraint), *citing Alexander v. United States*, 509 U.S. 544, 550 (1993) ("Temporary restraining orders and permanent injunctions—i.e., court orders that actually forbid speech activities—are classic examples of prior restraints."); *supra* §§ 4.13[1] (discussing the case), 6.16[1] (analyzing injunctive relief under the Lanham Act).

[59]*Petroliam Nasional Berhad v. GoDaddy.com, Inc.*, 737 F.3d 546, 550 (9th Cir. 2013); *see generally supra* §§ 7.06, 7.14, 7.21.

[60]*See, e.g.*, *Coach,Inc. v. Sapatis*, 994 F. Supp. 2d 192, 201-02 (D.N.H. 2014); *Coach, Inc. v. Swap Shop, Inc.*, 916 F. Supp. 2d 1271, 1280-82 (S.D. Fla. 2012); *Coach, Inc. v. Farmers Market & Auction*, 881 F. Supp. 2d 695, 705-06 (D. Md. 2012); *Microsoft Corp. v. Shah*, Case No. C10-0653 RSM, 2011 WL 108954, at *4 (W.D. Wash. Jan. 12, 2011).

[61]*See generally supra* § 6.11[6] (analyzing this issue).

[62]*See Societe Des Hotels Meridien v. LaSalle Hotel Operating Partnership, L.P.*, 380 F.3d 126, 131-32 (2d Cir. 2004) (reversing the district court's dismissal of plaintiff's claim for contributory false advertising—premised

although it is questionable whether such a theoretical claim in fact could be asserted[64] consistent with the requirement for proximate cause and statutory standing under the Supreme Court's decision in *Lexmark Int'l, Inc. v. Static Control Components, Inc.*[65]

Significant secondary liability cases are discussed at length in section 6.10[2].

The liability risks and exemptions of domain name registrars and registries are separately analyzed in section 7.21.

---

on Meridien's allegation that LaSalle induced Starwood to violate the Lanham Act "by intentionally directing, approving, authorizing, drafting and/or editing the Starwood Worldwide Directories"—in connection with reversing the district court's dismissal of plaintiff's claim for direct liability, without any discussion of whether such a claim in fact exists). *Meridien* involved only very brief treatment of the issue. It also pre-dates the Supreme Court's decision in *Lexmark*.

[63]*See Duty Free America, Inc. v. Estee Lauder Cos.*, 797 F.3d 1248, 1274-79 (11th Cir. 2015) (holding that a plaintiff who can state a claim for direct false advertising under *Lexmark*—by alleging (1) statements that were false or misleading, (2) which deceived, or had the capacity to deceive, (3) which deception had a material effect on consumers' purchasing decisions, (4) where the misrepresented service affects interstate commerce, and (5) where the plaintiff has been or will be injured as a result of the false or misleading statement—may state a claim for contributory liability by alleging that a defendant contributed to that conduct (that it "intended to participate in" or "actually knew about" the false advertising) and actively and materially furthered the unlawful conduct, either by inducing it, causing it or in some other way working to bring it about). The court in *Duty Free America* suggested that courts look to contributory trademark infringement case law for guidance, suggesting that the participation prong of a contributory false advertising claim could be met by alleging that a defendant directly controlled and monitored the third party's false advertising. *Id.* at 1277. The court also suggested that it was "conceivable that there could be circumstances under which the provision of a necessary product or service, without which the false advertising would not be possible, could support a theory of contributory liability." *Id.* at 1277-78. In affirming dismissal of plaintiff's claim, the appellate panel wrote that "[c]ontributory false advertising claims are cognizable under the Lanham Act, but a plaintiff must allege more than an ordinary business relationship between the defendant and the direct false advertiser in order to plausibly plead its claim." *Id.* at 1279.

[64]*See, e.g.*, *Academy of Doctors of Audiology v. Int'l Hearing Society*, 237 F. Supp. 3d 644, 666 (E.D. Mich. 2017) (dismissing plaintiff's claim for contributory false advertising).

[65]*Lexmark Int'l, Inc. v. Static Control Components, Inc.*, 134 S. Ct. 1377 (2014); *supra* § 6.12[5][F].

49.07 Right of Publicity Claims

The grounds for imposing secondary liability for a right of publicity violation are murky and, at least in some jurisdictions, claims would be preempted by the Good Samaritan exemption created by the Communications Decency Act. Some site owners and service providers nevertheless try to work out complaints received from rights owners even in the absence of any formal notice and takedown system. If in doubt, it is often safer for a site or service to remove material upon receipt of notice setting forth a colorable claim that a given use was unauthorized, unless the service provider is willing to litigate the dispute.

Violations of the rights of celebrities and others to control the commercial exploitation of their name, likeness and other personal attributes are potentially actionable to varying degrees under the federal Lanham Act (if protected like a trademark), state statutes (where enacted) and common law tort theories of recovery.[1] Publicity rights are akin to trademarks in a person's popular image. In the words of the U.S. Supreme Court, they are "closely analogous to the goals of patent and copyright law, focusing on the right of the individual to reap the rewards of his endeavors . . . ."[2] Publicity rights may be somewhat narrower than other forms of intellectual property,[3] however, because the protections afforded vary significantly from state to state,[4] the First Amendment limits the scope of individual protection in some cases involving third-party speech or press rights or public officials or figures,[5] and under certain circumstances claims may be preempted by the Copyright Act.[6]

An Internet site or service potentially could be held secondarily liable for a right of publicity violation involving user generated content if it received notice and failed to take

---

[Section 49.07]

[1]*See generally supra* §§ 12.01 to 12.07.

[2]*Zacchini v. Scripps-Howard Broadcasting Co.*, 433 U.S. 562, 573 (1977).

[3]Rights of publicity actually originated under state tort law and continue to be recognized as part of privacy law, even though they may be protected and licensed like copyrighted works or trademarks. *See supra* § 12.01.

[4]*See supra* §§ 12.01 to 12.03.

[5]*See supra* §§ 12.05[3], 12.05[4].

[6]*See supra* §§ 12.05[2], 12.06.

action, provided the claim was not preempted. Right of publicity law varies from state to state. Whether a claim for secondary liability *in fact* may be asserted successfully may turn on the specific terms of the applicable state right of publicity statute at issue (or construction of common law rights).

There is not much case law on secondary liability for right of publicity violations, but there is some limited authority for holding distributors or other intermediaries liable in circumstances where they have knowledge and fail to act.[7] It is also theoretically conceivable that liability could be imposed even without knowledge where state law does not require a showing of knowledge, such as under the California common law right of publicity,[8] although no court has yet imposed liability on this basis.

---

[7]*See Perfect 10, Inc. v. Cybernet Ventures, Inc.*, 213 F. Supp. 2d 1146 (C.D. Cal. 2002) (granting plaintiff's motion for a preliminary injunction based on the finding that the plaintiff was likely to prevail on its claim that the defendant could be held secondarily liable for a California statutory right of publicity violation based on common law theories of aiding and abetting and unfair competition); *see also Brinkley v. Casablancas*, 80 A.D.2d 428, 443–44, 438 N.Y.S.2d 1004 (1st Dep't 1981) (granting a motion to dismiss because a right of publicity claim against a vendor requires a showing of knowledge or at least notice that its exploitation of rights is unauthorized).

Other courts presented with a claim for secondary liability have avoided the specific question of whether a claim may be maintained. *See, e.g., Almeida v. Amazon.com, Inc.*, 456 F.3d 1316, 1324–26 (11th Cir. 2006) (affirming the entry of summary judgment for Amazon.com, holding that an Internet retailer could not be liable under Florida's right of publicity statute for displaying a book offered for sale on its website, where the book allegedly included an unauthorized photo on the cover, based on the court's construction of "commercial purpose" under the Florida statute, the incidental use exception and the court's conclusion that displaying a photo of a book cover online was equivalent to displaying a book in the window of a bookstore, which would not be actionable).

[8]A claim for a violation of a person's rights of publicity under California common law does not appear to require a showing of knowledge. *See Kirby v. Sega of America, Inc.*, 144 Cal. App. 4th 47, 55, 50 Cal. Rptr. 3d 607 (2d Dist. 2006) ("common law and statutory [appropriation] claims are similar but not identical . . . . A statutory cause of action for appropriation not only encompasses the common law elements, it requires a knowing use of the plaintiff's name, likeness, etc."); *Downing v. Abercrombie & Fitch*, 265 F.3d 994, 1001 (9th Cir. 2001) (holding that "[u]nder section 3344, a plaintiff must prove all the elements of the common law cause of action. In addition, the plaintiff must allege a knowing use by the defendant as well as a direct connection between the alleged use and the commercial purpose.").

Even if a claim may be stated against a site or service for user generated content under applicable state law, the claim may be preempted by the Good Samaritan exemption to the Telecommunications Act of 1996, otherwise known as the Communications Decency Act or CDA.[9] There is presently a split of authority over whether the Good Samaritan exemption preempts state law claims pertaining to intellectual property, including right of publicity claims.[10]

Rights of publicity claims may also arise under the Lanham Act. Not all publicity violations would qualify as Lanham Act claims—only those where the person has developed trademark rights in his or her name or likeness.[11] Where actionable, a party potentially could assert Lanham Act claims for contributory infringement and vicarious

---

To state a claim for a violation of common law rights under California law, a plaintiff generally must show:

(1) the defendant's use of the plaintiff's identity;

(2) the appropriation of plaintiff's name or likeness (or the impersonation of the plaintiff) to defendant's advantage, commercial or otherwise;

(3) lack of consent; and

(4) resulting injury (shown by traditional lost revenue or injury to reputation—such as when a mainstream entertainer is featured on an Internet porn site).

Michaels v. Internet Entertainment Group, Inc., 5 F. Supp. 2d 823, 838 (C.D. Cal. 1998).

[9]47 U.S.C.A. § 230(c); *supra* § 49.04.

[10]*Compare Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102 (9th Cir.) (construing the term "any law pertaining to intellectual property" to be restricted to "federal intellectual property" and therefore holding that the plaintiff's right of publicity claim against an Internet payment processor was preempted), *cert. denied,* 522 U.S. 1062 (2007) *with Doe v. Friendfinder Network, Inc.*, 540 F. Supp. 2d 288 (D.N.H. 2008) (holding that "any law pertaining to intellectual property" literally means any law—state or federal—and therefore denying the defendant's motion to dismiss plaintiff's right of publicity claim under New Hampshire law); *and Atlantic Recording Corp. v. Project Playlist, Inc.*, 603 F. Supp. 2d 690 (S.D.N.Y. 2009) (construing the literal language of the statute the same way as the court in *Doe* and allowing a common law copyright claim under New York law to proceed); *UMG Recordings, Inc. v. Escape Media Group, Inc.*, 948 N.Y.S. 881, 888–89 (N.Y. Sup. 2012) (same), *rev'd on other grounds*, 107 A.D.3d 51, 964 N.Y.S.2d 106 (N.Y. App. 2013); *supra* § 49.04; *see generally supra* § 37.05[5][B] (analyzing the issue in greater detail and discussing more recent case law).

[11]*See supra* § 12.03[3].

liability.[12] A claim for secondary liability under the Lanham Act would not be deemed preempted by the Good Samaritan exemption[13] and would be evaluated under the standards (and subject to the defenses, including the innocent printer's and publisher's defense) set forth in section 49.06.

In *Perfect 10, Inc. v. Cybernet Ventures, Inc.*,[14] Judge Lourdes Baird of the Central District of California held that an adult verification service could be held secondarily liable for a violation of California's right of publicity statute, based on principles of aiding and abetting liability, as set forth in the Restatement (Second of Torts). In that case, the court construed Cal. Civil Code § 3344(f), which created a heightened knowledge requirement for imposing liability on owners or employees of any medium used for advertising (such as newspapers and television stations), as evidencing a legislative intent that secondary liability for right of publicity violations was permissible under California law (albeit with a heightened showing of proof of knowledge when the defendant is a broadcaster of advertisements).

In *Cybernet*, the court held that the defendant was not a broadcaster, and therefore could be subject to secondary liability based on the regular showing required to state a claim under section 3344, provided the elements of aiding and abetting liability could be shown. Under the Restatement, liability may be imposed for harm resulting to a third person from the tortious conduct of another if it: (a) does a tortious act in concert with the other in pursuit of a common design; (b) knows that the other's conduct constitutes a breach of duty and gives substantial assistance or encouragement; or (c) gives substantial assistance to the other in accomplishing a tortious result and its own conduct, separately considered, constitutes a breach of a duty to a third person.[15]

Cybernet would be decided differently today, at least in the same court that originally rendered the decision, because since the time it was decided the Ninth Circuit ruled that the Good Samaritan exemption preempts right of publicity claims brought against interactive computer service provid-

---

[12]*See supra* § 49.06.

[13]47 U.S.C.A. § 230(e)(2).

[14]*Perfect 10, Inc. v. Cybernet Ventures, Inc.*, 213 F. Supp. 2d 1146 (C.D. Cal. 2002).

[15]*Perfect 10, Inc. v. Cybernet Ventures, Inc.*, 213 F. Supp. 2d 1146, 1183 (C.D. Cal. 2002), *citing* Restatement (Second) of Torts § 876.

ers for content originating with another information content provider.[16] Nevertheless, it is possible that a California state court could rely on *Cybernet* for the proposition that secondary liability may be imposed under California law for a right of publicity violations but not find the claim preempted (since federal district court decisions construing state law are not binding on state courts). It is also possible that a court in another jurisdiction could find *Cybernet* to be persuasive authority. To date, however, no other court has followed *Cybernet*'s holding.

Even where the Good Samaritan exemption may be found inapplicable, some courts may be reluctant to hold site owners or service providers liable for privacy and publicity violations by their users (as distinguished from suits against the users themselves).[17] In *Doe v. GTE Corp.*,[18] for example, the Seventh Circuit affirmed dismissal of a suit brought by college athletes who were secretly video-recorded in locker rooms, bathrooms and showers, against the companies that provided Internet access and Web hosting services to sites that sold copies of these videos. The court found that plaintiffs had not shown that the Web hosting company defendants had any legal obligation under applicable state law to investigate their clients' activities and cut off those customers who were selling hurtful materials and the plaintiffs could not state claims under the Electronic Communications Privacy Act.[19]

In *Perfect 10, Inc. v. Visa Int'l Service Ass'n*,[20] the Ninth Circuit affirmed dismissal of claims for vicarious liability under California's unfair competition, false advertising and right of publicity laws for infringing images sold by websites that used Visa for payment processing services for the transactions because Visa "lack[ed] sufficient control or personal involvement in the infringing activities to be [held]

---

[16]*See Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102 (9th Cir.), *cert. denied,* 522 U.S. 1062 (2007).

[17]It is often difficult to know who the person responsible is when material is posted online. Satellite litigation to compel the disclosure of the identity of anonymous or pseudonymous Internet tortfeasors or infringers often must be brought. *See supra* § 37.02.

[18]*Doe v. GTE Corp.*, 347 F.3d 655 (7th Cir. 2003).

[19]18 U.S.C.A. §§ 2511, 2520.

[20]*Perfect 10, Inc. v. Visa Int'l Service Ass'n*, 494 F.3d 788 (9th Cir. 2007), *cert. denied*, 553 U.S. 1079 (2008).

liable."[21]

Similarly, in *Parisi v. Sinclair*,[22] even though the court declined "to extend the scope of the CDA immunity as far as the Ninth Circuit . . . ," it nonetheless dismissed plaintiff's right of publicity claim as barred by the newsworthiness exception (which is separately analyzed in section 12.05[4][B]). In that case, the porn industry owner of WhiteHouse.Com had sued Sinclair and various booksellers over various assertions Sinclair had made in promotional material and elsewhere for a book allegedly detailing his experiences taking drugs with then-Presidential candidate Barak Obama.

In *Gauck v. Karamian*,[23] the court assumed, for purposes of plaintiff's motion for a preliminary injunction, that plaintiff's publicity rights claim fell within the CDA's statutory exclusion for claims that arise "from any law pertaining to intellectual property" but nonetheless denied the motion based on the plaintiff's inability to show she was likely to prevail on the merits, at least at that stage in the proceedings. The plaintiff, a local television news reporter, had sued the owners of DirtyWorld.Com, which solicited user material and added its own commentary to the material. Plaintiff objected to posts of photos of herself (as well as photos of a naked woman falsely attributed to her) and related commentary, which she alleged was used by defendants to advertise and draw additional traffic to the site. Tennessee's right of publicity statute, in contrast to many others, proscribes only unauthorized use of another's name or likeness in advertising.[24] In denying plaintiff's motion, the court noted that the plaintiff had "suggested, at most, a currently unsubstantiated connection between the general use of celebrity personas on the site and an increase in traffic and/or advertising revenue."[25]

Additional cases are analyzed in section 12.04.

---

[21]*Perfect 10, Inc. v. Visa Int'l Service Ass'n*, 494 F.3d 788, 809 (9th Cir. 2007), *cert. denied*, 553 U.S. 1079 (2008).

[22]*Parisi v. Sinclair*, 774 F. Supp. 2d 310 (D.D.C. 2011).

[23]*Gauck v. Karamian*, 805 F. Supp. 2d 495 (W.D. Tenn. 2011).

[24]Tenn. Code Ann. § 27-25-1105(a); *Gauck v. Karamian*, 805 F. Supp. 2d 495, 500–01 (W.D. Tenn. 2011).

[25]*Gauck v. Karamian*, 805 F. Supp. 2d 495, 503 (W.D. Tenn. 2011).

49.08 Trade Secret Misappropriation

Congress, in enacting the Defend Trade Secrets Act (DTSA),[1] made clear that any claim against an interactive computer service provider or user based on secondary liability potentially could be precluded by the Good Samaritan exemption created by the Communications Decency Act, and could not be excluded from potential CDA immunity as a matter "pertaining to intellectual property."[2] By contrast, a claim brought for misappropriation of trade secrets under state law, like other state law IP claims,[3] may or may not be subject to CDA immunity, depending on where suit is filed. At the same time, the grounds for imposing trade secret liability on a site owner or service provider for user conduct or content appear limited.

There are no specific doctrines of vicarious trade secret liability analogous to those recognized under copyright, trademark and patent law.[4] As a general rule, a platform may not be held vicariously (or secondarily) liable for destroying a trade secret publicly posted by a user. Indeed, courts thus far have uniformly rejected claims brought against service providers whose users, customers or subscribers allegedly disclosed trade secrets in violation of duties owed to plaintiffs.[5] Similarly, accessing a trade secret once it

---

[Section 49.08]

[1]18 U.S.C.A. §§ 1830 to 1839; *see generally supra* § 10.12[2] (analyzing the statute).

[2]47 U.S.C.A. §§ 230(c), 230(e)(2); 18 U.S.C.A. §§ 1833 note, 1836 note, 1839 note; Pub L. 114-153 § 2(g), 130 Stat. 376, 382 (2016) ("This section and the amendments made by this section shall not be construed to be a law pertaining to intellectual property for purposes of any other Act of Congress."). This specific provision of the DTSA was codified as a note to sections 1833, 1836 and 1839. *See generally supra* § 37.05[5][B] (analyzing the interplay between the CDA and DTSA).

[3]*See supra* § 49.04 (outlining the IP exclusion set forth in the Good Samaritan provision).

[4]*See supra* §§ 49.05 (inducement and direct, contributory and vicarious copyright infringement), 49.06 (contributory and vicarious trademark infringement); *infra* § 49.09 (inducement and contributory patent infringement).

[5]*See, e.g., Religious Technology Center v. Netcom On-Line Communication Services, Inc.*, 923 F. Supp. 1231 (N.D. Cal. 1995); *Religious Technology Center v. F.A.C.T.NET, Inc.*, 901 F. Supp. 1519 (D. Colo. 1995); *Religious Technology Center v. Lerma*, 897 F. Supp. 260 (E.D. Va. 1995); *see also Ford Motor Co. v. Lane*, 67 F. Supp. 2d 745 (E.D. Mich. 1999)

has been publicly disclosed would not be actionable.[6] However, under limited circumstances in some jurisdictions, liability potentially could be imposed based on notice that a trade secret has been posted on a site or service and the failure to take action to remove it. In some jurisdictions, this claim could be preempted by the Good Samaritan exemption to the Telecommunications Act of 1996.[7]

Liability for trade secret misappropriation may be imposed under the Uniform Trade Secrets Act where a person knows or has *reason to know* that material was acquired through improper means,[8] or was derived from such material, constitutes a trade secret, and was made available by accident or mistake, or was obtained from someone who was under a duty to keep it confidential.[9] Liability in such cases would be

---

(declining to enjoin a website's publication of plaintiff's trade secrets on the grounds that such an order would constitute an impermissible prior restraint); *see generally supra* § 10.11.

[6]*See, e.g., Religious Technology Center v. Lerma*, 908 F. Supp. 1362, 1368 (E.D. Va. 1995) ("Although the person who originally posted a trade secret on the Internet may be liable for trade secret misappropriation, the party who merely downloads Internet information cannot be liable for misappropriation because there is no misconduct involved in interacting with the Internet."); *DVD Copy Control Ass'n Inc. v. Bunner*, 116 Cal. App. 4th 241, 10 Cal. Rptr. 3d 185 (6th Dist. 2004) (reversing entry of a preliminary injunction where the alleged trade secret was widely disseminated on the Internet).

[7]47 U.S.C.A. § 230(c); *see generally supra* § 37.05[5][B] (analyzing the issue in substantially greater detail).

[8]*See* UTSA § 1(2)(i) (emphasis added); *DVD Copy Control Ass'n, Inc. v. Bunner*, 31 Cal. 4th 864, 4 Cal. Rptr. 3d 69 (2003) (holding that a preliminary injunction could be entered against a site owner on this basis). In *Bunner*, the site owner himself posted the secret and, on subsequent appeal after remand, an intermediate appellate court ruled that an injunction could not enter because the secret was so widely available on the Internet. The California Supreme Court's 2003 opinion, however, establishes the principle that liability may be imposed under California law where a site owner or service provider comes into possession of a trade secret where a person knows or has reason to know that material was acquired through improper means.

[9]*See* UTSA § 1(2); *supra* § 10.12. Similarly, under Texas law, a defendant was held liable for trade secret misappropriation where it duped a third party into providing it with a copy of plaintiff's operating system software in violation of his confidentiality agreement with the plaintiff, which it then used to disassemble plaintiff's firmware. Although the defendant itself had no contractual or confidentiality obligations to the plaintiff (and disassembly or reverse engineering otherwise is not prohibited by trade secret law), it was held to have used improper means

premised on actual or imputed knowledge. Mere notice in most cases should be insufficient to confer *knowledge*, since a platform typically is not in a position to evaluate technical claims.[10]

Nevertheless, even if such a claim were viable, it could be preempted by the Good Samaritan exemption to the Telecommunications Act of 1996.[11] The exemption provides broad immunity for providers and users of *interactive computer services* (which is expansively defined to cover most websites, blogs, ISPs, social networks, employer networks or other interactive computer networks) from content originating with third parties (such as user content). The statute broadly preempts civil claims arising under state law, but excludes claims "pertaining to intellectual property."[12] There presently is conflicting authority on whether the exemption applies to or excludes state intellectual property claims, such as a trade secret claim under state law, as opposed to a federal claim, under the Defend Trade Secrets Act (even though both state and federal claims may be joined together in a single action).

---

to acquire plaintiff's trade secrets in its firmware by unlawfully obtaining a copy of the operating system, which was necessary to understanding plaintiff's firmware. *See Alcatel USA, Inc. v. DGI Technologies, Inc.*, 166 F.3d 772, 784–85 (5th Cir. 1999).

[10]*See, e.g.*, *Blazer v. eBay, Inc.*, Case No. 1:15-cv-01059-KOB, 2017 WL 1047572, at *5 (N.D. Ala. Mar. 20, 2017) (granting summary judgment for eBay because eBay did not have knowledge of patent infringement merely because plaintiff notified eBay of its claims); *see generally infra* § 49.09 (analyzing the *Blazer* case).

The mere assertion of a trade secret—like an allegation of patent infringement or a claim of trademark infringement based on the likelihood of consumer confusion—is difficult if not impossible for a platform provider to fairly evaluate. Notice to a platform provider therefore should not be construed as the same thing as *knowledge*. *See, e.g.*, *Lockheed Martin Corp. v. Network Solutions, Inc.*, 985 F. Supp. 949, 951 (C.D. Cal. 1997) (referring to the obligations of a registrar in accepting domain name registrations), *aff'd*, 194 F.3d 980 (9th Cir. 1999); *see generally supra* § 6.10.

[11]47 U.S.C.A. § 230(c).

[12]47 U.S.C.A. § 230(e)(2). A state law trade secret claim arguably "pertain[s] to intellectual property." Nevertheless, the Supreme Court has adopted the definition of a trade secret taken from the Restatement of Torts, implicitly recognizing trade secret protection as a creature of state tort law. *See, e.g., Bonito Boats, Inc. v. Thunder Craft Boats, Inc.*, 489 U.S. 141 (1989); *Aronson v. Quick Point Pencil Co.*, 440 U.S. 257 (1979); *see supra* §§ 10.02, 10.05.

In *Perfect 10, Inc. v. ccBill, Inc.*,[13] the Ninth Circuit construed the term "intellectual property" to mean "federal intellectual property" and ruled that the plaintiff's California state right of publicity claim against an Internet payment processor was preempted.[14] Based on *Perfect 10*, trade secret claims brought against third parties would be deemed preempted in the Ninth Circuit.[15] The reasoning of *Perfect 10*, however, was criticized in *Doe v. Friendfinder Network, Inc.*,[16] a district court decision from New Hampshire, in which Judge Joseph N. LaPlante denied the defendant's motion to dismiss a state right of publicity claim, finding the statutory exclusion for *any* claim pertaining to intellectual property was not restricted to federal IP claims as the Ninth Circuit had held. Under the analysis of *Friendfinder Network* (and cases from the Southern District of New York and New York state court decided on similar grounds)[17] trade secret claims against third parties would *not* be preempted by the Good Samaritan exemption. These issues are addressed in greater detail in sections 10.18 and 37.05[5][B].

If a site owner or service provider receives credible notice of an alleged trade secret posted on its site or service, the prudent response would be to swiftly disable access to or remove the material. Even if the notice might not be suf-

---

[13]*Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102 (9th Cir.), *cert. denied,* 522 U.S. 1062 (2007).

[14]*Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102, 1118–19 (9th Cir.), *cert. denied,* 522 U.S. 1062 (2007).

[15]*See, e.g.*, *Stevo Design, Inc. v. SBR Mktg. Ltd.*, 919 F. Supp. 2d 1112, 1127 (D. Nev. 2013) (dismissing plaintiff's complaint with leave to amend; holding that a sports betting website operator was immune from Florida law claims for misappropriation of trade secrets and common law misappropriation of licensable commercial property because it was not a "developer" of user-generated content under the CDA, even though it awarded loyalty points for user posts). *But see Stevo Design, Inc. v. SBR Mktg. Ltd.*, 968 F. Supp. 2d 1082, 1090–91 (D. Nev. 2013) (denying defendant's motion to dismiss plaintiff's amended trade secret and common law misappropriation claims, which sought to plead around the CDA); *see generally supra* § 37.05[5][B] (analyzing the issue more extensively).

[16]*Doe v. Friendfinder Network, Inc.*, 540 F. Supp. 2d 288 (D.N.H. 2008).

[17]*See Atlantic Recording Corp. v. Project Playlist, Inc.*, 603 F. Supp. 2d 690, 702-04 (S.D.N.Y. 2009) (construing the literal language of the statute the same way as the court in *Doe* and allowing a common law copyright claim under New York law to proceed); *UMG Recordings, Inc. v. Escape Media Group, Inc.*, 948 N.Y.S. 881, 888–89 (N.Y. Sup. 2012) (same), *rev'd on other grounds*, 107 A.D.3d 51, 964 N.Y.S.2d 106 (N.Y. App. 2013).

ficient to cause the recipient to be deemed to have knowledge (because it is usually almost impossible for a service provider to evaluate the merits of an alleged trade secret misappropriation claim based solely on notice), the potential risk that it could be found sufficient to provide *reason to know*, and therefore at the very least a duty to investigate (in those states where failure to do so could be actionable), makes it prudent for a platform provider to respond when provided with notice (especially in places where the CDA may not afford a complete defense). Many sites and services consider it prudent to investigate and take seriously allegations that trade secrets have been posted online.

49.09 Direct, Contributory and Inducing Patent Infringement

49.09[1] In General

Intent is not an element of a claim for patent infringement,[1] except where liability is premised on inducement or contributory patent infringement. In general, patent holders may exclude others from practicing a claimed invention, regardless of whether the defendant even knew it was infringing a patent.[2] Patent liability may be imposed where an owner or provider directly infringed a patent (such as one covering software or Internet business methods or used infringing hardware to provide service). Liability may be imposed for user (or other third party) conduct or content based on contributory infringement or inducement, but only where knowledge or intent are shown. As discussed below, the grounds for imposing secondary patent liability on site owners or service providers for the acts of their users are narrower than under copyright law[3] and, unlike copyright law, are based on specific statutory provisions.

Although the risk of liability for the conduct of users may be limited, the prevalence of trolls, the fact that a patent may issue long after an application has been filed, and the increasing number of software and business method patents that issued after the Federal Circuit's 1998 decision in *State*

[Section 49.09[1]]

[1] E.g., *Kewanee Oil Co. v. Bicron Corp.*, 416 U.S. 470, 478 (1974).

[2] *See supra* § 8.09[2].

[3] *See supra* § 49.05.

Street Bank & Trust Co. v. Signature Financial Group, Inc.[4] and before the Court again tightened restrictions on patentability, make it difficult to evaluate the potential patent risks associated with an e-commerce site.[5] In a sense today, being sued by a patent troll is a cost of doing business that every Internet site or service should anticipate. Site owners and service providers therefore often seek patent indemnifications in connection with business deals, although for these same reasons business partners may be reluctant to provide them. These same uncertainties may make insurance difficult or expensive to obtain.

49.09[2] Direct Liability for Patent Infringement

Direct liability for patent infringement may be established by evidence that a defendant, without authority, "makes, uses or sells any patented invention, within the United States during the term of the patent . . . ."[1] Liability for patent infringement also may be based on importation (or offers of sale) of products manufactured abroad by processes protected in the United States by process patents[2] or imposed for supplying component parts to be assembled abroad in a manner that would constitute patent infringement if so combined in the United States.[3]

49.09[3] Contributory Patent Infringement

Liability for contributory patent infringement must be premised on knowledge.[1] Notice to a site owner or service provider, while potentially evidence, does not itself constitute knowledge. Moreover, the scope of contributory liability

---

[4]*State Street Bank & Trust Co. v. Signature Financial Group, Inc*, 149 F.3d 1368 (Fed. Cir. 1998).

[5]*See supra* § 8.04.

[Section 49.09[2]]

[1]35 U.S.C.A. § 271(a).

[2]35 U.S.C.A. § 271(g).

[3]35 U.S.C.A. § 271(f).

[Section 49.09[3]]

[1]In a case construing inducement under 35 U.S.C.A. § 271(b), the U.S. Supreme Court held that knowledge for purposes of proving inducement is the same as what is required to show contributory infringement under section 271(c), namely "knowledge of the existence of the patent that is infringed." *Global-Tech Appliances, Inc. v. SEB S.A.*, 563 U.S. 754, 765 (2011).

is narrower than under copyright law[2] and limited to sales, offers of sales or imports of components of patented machines or material or apparatus for use in practicing a patented process, and even then under limited circumstances. As with secondary copyright or trademark infringement, there must be an underlying act of direct patent infringement or else there can be no liability for contributory infringement.[3]

Contributory patent infringement is codified in 35 U.S.C.A. § 271(c), which provides that:

> Whoever offers to sell or sells within the United States or imports into the United States a component of a patented machine, manufacture, combination or composition, or a material or apparatus for use in practicing a patented process, constituting a material part of the invention, knowing the same to be especially made or especially adapted for use in an infringement of such patent, and not a staple article or commodity of commerce suitable for substantial noninfringing use, shall be liable as a contributory infringer.[4]

Section 271(c) requires "proof of a defendant's *knowledge*, not *intent*, that his activity cause[s] infringement . . . ."[5] It compels a showing of "not only knowledge that the component [or apparatus for use in a patented process] was especially made or adapted for a particular use but also knowledge of the patent which proscribed that use."[6] A subjective belief of infringement is not a necessary element. "All that is required for a finding of contributory infringement is (1) knowledge of the activity that is alleged to be infringing . . . , and (2) knowledge of the patent."[7]

A patent owner seeking to hold a site owner or service

---

[2] *See supra* § 49.05[3][C].

[3] *Aro Mfg. Co. v. Convertible Top Replacement Co.*, 365 U.S. 336, 341–42 (1961); *Molinaro v. Fannon/Courier Corp.*, 745 F.2d 651, 654 (Fed. Cir. 1984).

[4] 35 U.S.C.A. § 271(c).

[5] *Hewlett-Packard Co. v. Bausch & Lomb Inc.*, 909 F.2d 1464, 1469 (Fed. Cir. 1990) (emphasis in original).

[6] *Hewlett-Packard*, 909 F.2d at 1469 n.4, *citing Aro Mfg. Co. v. Convertible Top Replacement Co.*, 377 U.S. 476, 488 (1964).

[7] *Sandisk Corp. v. Lexar Media, Inc.*, 91 F. Supp. 2d 1327, 1334 (N.D. Cal. 2000) (noting that there is no requirement that a defendant subjectively believe that its use of a device infringes a patent); *see also Nordberg Mfg. Co. v. Jackson Vibrators, Inc.*, 153 U.S.P.Q. 777, 784–85, 1967 WL 7708 (N.D. Ill. 1967) (noting that if subjective belief of infringement were required for a finding of contributory infringement, an infringer would be insulated from liability made prior to a final judgment of

provider liable for third-party conduct or content likely would seek to place it on notice of the alleged infringement. Notice of claimed infringement or a cease and desist letter may be introduced as evidence of knowledge for purposes of proving contributory infringement.[8] A cease and desist letter or notice alone, however, may not be sufficient to actually prove the knowledge required for contributory liability absent other evidence.[9] Actual knowledge under the Patent Act arguably is different from mere notice,[10] at least in most instances.

---

infringement), *rev'd on other grounds*, 393 F.2d 192 (7th Cir. 1968).

[8]*See, e.g., Aro Mfg. Co. v. Convertible Top Replacement Co.*, 377 U.S. 476, 489 (1964) (holding that a letter notifying the seller of the patent and a claim of infringement constituted evidence of knowledge); *Fuji Photo Film Co. v. Jazz Photo Corp.*, 394 F.3d 1368, 1378 (Fed. Cir. 2005) (finding intent based in part on evidence that the defendant was aware of plaintiff's infringement contentions); *Mentor H/S, Inc. v. Medical Device Alliance, Inc.*, 244 F.3d 1365, 1379 (Fed. Cir. 2001) (finding that the defendant knew of the existence of the patent in part because it received a cease-and-desist letter concerning it); *Ocean Innovations, Inc. v. Archer*, 483 F. Supp. 2d 570, 583 (N.D. Ohio 2007) (holding the defendant contributorily liable in part because "plaintiffs have shown that defendant knew of the '833 patent at least since the notice letters were sent.").

[9]*See, e.g., MEMC Electronic Materials, Inc. v. Mitsubishi Materials Silicon Corp.*, 420 F.3d 1369, 1380 (Fed. Cir. 2005) (finding that the defendant knew of the existence of the '302 patent because it received a letter concerning it but noting in *dicta* that while this type of evidence is relevant to establish intent, it is "not by itself sufficient.").

[10]*See Blazer v. eBay, Inc.*, Case No. 1:15-cv-01059-KOB, 2017 WL 1047572, at *5 (N.D. Ala. Mar. 20, 2017) (granting summary judgment for eBay because eBay did not have knowledge of infringement merely because plaintiff notified eBay of its claims); *Celanese International Corp. v. Oxyde Chemicals, Inc.*, 554 F. Supp. 2d 725, 729 (S.D. Tex. 2008). In *Celanese*, the defendant argued that it was entitled to have the available remedies limited by section 287, which states that remedies for infringement under section 271(g) (infringement by importation) are unavailable prior to the time an alleged infringer has "notice" of infringement. Section 287's limitation is not available, however, to any person who "had knowledge before the infringement that a patented process was used to make the product the importation, use, offer for sale, or sale of which constitutes the infringement." 35 U.S.C.A. § 287(b)(1)(C). While the defendant had received written notice of the alleged infringement before the sale of the allegedly infringing product, the court found that such notice did not provide the level of "knowledge" required under section 287(b)(1)(C) because there was no evidence that the defendant knew that the allegedly infringing product was produced in a manner covered by the allegedly infringed process patent. *Celanese*, 554 F. Supp. 2d at 729. The court noted in particular that section 287(b)(5)(A) specifically defines notice to mean "either actual knowledge or receipt of written notification, indicat-

This point was underscored in *Blazer v. eBay, Inc.*,[11] a case in which the court determined that eBay, the online marketplace, was neither liable for direct nor secondary infringement (based on either contributory infringement or inducement) for various carpenter bee traps sold by users of its online marketplace, even though the plaintiff had provided notice of alleged infringement. eBay, consistent with its policies, did not remove any of the allegedly infringing listings based simply on an assertion of patent infringement, but informed the plaintiff that it would honor a court order if a court agreed that the accused products were infringing.[12]

With respect to direct liability, the court granted summary judgment for eBay, holding that it did not offer for sale or sell the products listed for sale by users of its website.[13] Chief Judge Karon Owen Bowdre of the Northern District of Alabama explained that "no reasonable consumer could conclude that by bidding on an eBay listing, he was accepting an offer from eBay itself. eBay's terms of service explicitly advise users that eBay is not making an offer through a listing, and . . . eBay lacks title and possession of the items listed."[14]

For this same reason, Judge Bowdre held that eBay could

---

ing that knowledge and notice are not synonymous," and stated that "[a]ctual knowledge is sufficient for notice, but notice may not necessarily constitute knowledge." *Celanese*, 554 F. Supp. 2d at 729 While this case dealt with a different provision of the Patent Act than 271(c), the standard for what constitutes knowledge, as opposed to mere notice, arguably is relevant by analogy.

[11] *Blazer v. eBay, Inc.*, Case No. 1:15-cv-01059-KOB, 2017 WL 1047572 (N.D. Ala. Mar. 20, 2017).

[12] *See Blazer v. eBay, Inc.*, Case No. 1:15-cv-01059-KOB, 2017 WL 1047572, at *6 (N.D. Ala. Mar. 20, 2017).

[13] *Blazer v. eBay, Inc.*, Case No. 1:15-cv-01059-KOB, 2017 WL 1047572, at *2-5 (N.D. Ala. Mar. 20, 2017).

[14] *Blazer v. eBay, Inc.*, Case No. 1:15-cv-01059-KOB, 2017 WL 1047572, at *4 (N.D. Ala. Mar. 20, 2017). To "offer to sell" a product, a defendant must "communicate a manifestation of willingness to enter into a bargain, so made as to justify another person in understanding that his assent to that bargain is invited and will conclude" it. *MEMC Elec. Materials, Inc. v. Mitsubishi Materials Silicon Corp.*, 420 F.3d 1369, 1376 (Fed. Cir. 2005); *Rotec Industries, Inc. v. Mitsubishi Corp.*, 215 F.3d 1246, 1257 (Fed. Cir. 2000) (quoting Restatement (Second) of Contracts § 24 (1979)).

A "sale" for purposes of section 271(a) is determined according to the ordinary meaning of that term. *NTP, Inc. v. Research in Motion, Ltd.*, 418 F.3d 1282, 1319 (Fed. Cir. 2005) (citing Black's Law Dictionary 1337 (7th ed. 1999)), *abrogated on other grounds*, *Zoltek Corp. v. United States*, 672 F.3d 1309, 1323 (Fed. Cir. 2012) (*en banc*); *see also Halo Electronics,*

not be held liable for contributory infringement under section 271(c), which imposes liability for offering to sell or selling a patented product.[15] In addition, the court held that eBay did not "know that the product being sold infringed a patent" merely because the plaintiff repeatedly notified eBay of its claims.[16] Judge Bowdre—in an earlier part of the opinion which she cross referenced in her discussion of contributory infringement—explained that simply because eBay had received Notices of Claimed Infringement (NOCI) from the plaintiff did not evidence actual knowledge.[17] The court explained that although it was undisputed that the plaintiff had "communicated with eBay multiple times concerning the allegedly infringing products (including sending a copy of the patent to eBay), submitted multiple NOCI forms, and directly contacted eBay users who listed products he believed to infringe his patent" this was not sufficient for the plaintiff to avoid summary judgment because knowledge of a patent owner's *claims* is different from "*actual* knowledge of *infringement*."[18]

Blazer is discussed more extensively in section 8.10[2].

In another case involving an e-commerce selling platform, *Milo & Gabby, LLC v. Amazon.com*,[19] the district court affirmed a jury finding that Amazon.com was not liable for "of-

---

Inc. v. Pulse Electronics, Inc., 769 F.3d 1371, 1379 (Fed. Cir. 2014), *vacated on other grounds*, 136 S. Ct. 1923 (2016). "[T]he ordinary meaning of a sale includes the concept of a transfer of title or property." *Halo*, 769 F.3d at 1379 (quoting *NTP*, 418 F.3d at 1282); *see also, e.g.*, *PharmaStem Therapeutics, Inc. v. Viacell, Inc.*, 491 F.3d 1342, 1357 (Fed. Cir. 2007) (holding that "the transaction between the defendants and their clients is plainly not [a] sale" because "the defendants were never owners" of the product and "were not free to dispose of [it] as they chose."); U.C.C. § 2-106 ("A 'sale' consists in the passing of title from the seller to the buyer for a price.").

[15]*Blazer v. eBay, Inc.*, Case No. 1:15-cv-01059-KOB, 2017 WL 1047572, at *7 (N.D. Ala. Mar. 20, 2017), *quoting* 35 U.S.C.A. § 271(c).

[16]*Blazer v. eBay, Inc.*, Case No. 1:15-cv-01059-KOB, 2017 WL 1047572, at *7 (N.D. Ala. Mar. 20, 2017). The court addressed contributory infringement in summary form, incorporating by reference earlier parts of its opinion that had addressed "offer for sale" and knowledge (in the context of plaintiff's inducement claims).

[17]*Blazer v. eBay, Inc.*, Case No. 1:15-cv-01059-KOB, 2017 WL 1047572, at *5 (N.D. Ala. Mar. 20, 2017).

[18]*Blazer v. eBay, Inc.*, Case No. 1:15-cv-01059-KOB, 2017 WL 1047572, at *5 (N.D. Ala. Mar. 20, 2017) (emphasis in original).

[19]*Milo & Gabby, LLC v. Amazon.com*, 144 F. Supp. 3d 1251 (W.D.

fering to sell" products that allegedly infringed the plaintiffs' design patents.[20] In that case, Amazon had stipulated that the accused product design was substantially similar to those covered by the patents, but denied infringement, arguing that it did not make any "offer to sell" the products, which were made available for sale by third party users of Amazon's platform.[21] The district court had earlier determined that those third-party sellers—not Amazon—were responsible for providing the allegedly infringing products and that Amazon itself had not sold any of those products.[22] Following a three day trial, the jury found that Amazon did not "offer to sell" the products, concluding that Amazon did not communicate or provide a product description, a price, a quantity, or express any willingness to enter into a contract for sale of any of the products.[23] By adopting the jury's finding, the district court concluded that Amazon did not infringe the design patents.[24] The court's ruling was affirmed on appeal on other grounds.[25]

Contributory infringement may not be imposed for the sale of a "staple" article of commerce susceptible of substantial noninfringing use.[26]

Even where liability may be shown, damages potentially

Wash. 2015), *aff'd on other grounds*, 693 F. App'x 879 (Fed. Cir.), *cert. denied*, 138 S. Ct. 335 (2017).

[20]*Milo & Gabby, LLC v. Amazon.com*, 144 F. Supp. 3d 1251, 1251 (W.D. Wash. 2015), *aff'd on other grounds*, 693 F. App'x 879 (Fed. Cir.), *cert. denied*, 138 S. Ct. 335 (2017).

[21]*Milo & Gabby, LLC v. Amazon.com*, 144 F. Supp. 3d 1251, 1251-52 (W.D. Wash. 2015), *aff'd on other grounds*, 693 F. App'x 879 (Fed. Cir.), *cert. denied*, 138 S. Ct. 335 (2017).

[22]*Milo & Gabby, LLC v. Amazon.com*, 144 F. Supp. 3d 1251, 1252 (W.D. Wash. 2015), *aff'd on other grounds*, 693 F. App'x 879 (Fed. Cir.), *cert. denied*, 138 S. Ct. 335 (2017).

[23]*Milo & Gabby, LLC v. Amazon.com*, 144 F. Supp. 3d 1251, 1253 (W.D. Wash. 2015), *aff'd on other grounds*, 693 F. App'x 879 (Fed. Cir.), *cert. denied*, 138 S. Ct. 335 (2017).

[24]*Milo & Gabby, LLC v. Amazon.com*, 144 F. Supp. 3d 1251, 1253-54 (W.D. Wash. 2015), *aff'd on other grounds*, 693 F. App'x 879 (Fed. Cir.), *cert. denied*, 138 S. Ct. 335 (2017).

[25]*Milo & Gabby, LLC v. Amazon.com*, 693 F. App'x 879 (Fed. Cir.), *cert. denied*, 138 S. Ct. 335 (2017).

[26]*See* 35 U.S.C.A. § 271(c); *Dynacore Holdings Corp. v. U.S. Philips Corp.*, 363 F.3d 1263, 1275–76 n.6 (Fed. Cir. 2004); see *also supra* §§ 4.10[5], 4.11[1][F] (analyzing substantial noninfringing use under copyright law).

may be limited. The Supreme Court has held that the knowledge requirement of section 271(c) limits an alleged contributory infringer's liability to sales made *after* it received a letter from the patent holder informing it of the existence of the patent.[27] A site owner or service provider therefore may mitigate its exposure by simply discontinuing a disputed practice upon receiving notice or acquiring knowledge.

Contributory patent infringement is analyzed in greater detail in section 8.10[2].

49.09[4] Inducement

Inducement, like contributory infringement, is codified in the Patent Act. 35 U.S.C.A. § 271(b) provides that "[w]hoever actively induces infringement of a patent shall be liable as an infringer." Liability for active inducement is premised on aiding and abetting an infringer[1] and therefore requires a showing of intent. Liability may be established by evidence that (1) the defendant knowingly intended to induce another to infringe, and (2) there was an actual act of infringement by a third party (i.e., an underlying act of direct infringement).[2] The knowledge required to show inducement is "knowledge of the existence of the patent that is infringed" and "knowledge that the induced acts constitute patent infringement."[3] Knowledge, in turn, may be shown through evidence of actual knowledge or willful blindness.[4] Where liability for inducement is found, a third party may be held liable to the same extent as a direct infringer.[5]

The specific intent necessary to induce infringement "requires more than just intent to cause the acts that produce direct infringement . . . . [T]he inducer must have an

---

[27] *Aro Mfg. Co. v. Convertible Top Replacement Co.*, 377 U.S. 476, 491 (1964); *see also Trell v. Marlee Electronics Corp.*, 912 F.2d 1443, 1447 (Fed. Cir. 1990) (holding that defendant could be liable for damages only from the date it first obtained knowledge of plaintiff's patent).

[Section 49.09[4]]

[1] *See* S. Rep. No. 1979, 82d Cong., 2d Sess., *reprinted in* 1952 U.S.C. C.A.N. 2394, 2421.

[2] *Symantec Corp. v. Computer Associates Int'l, Inc.*, 522 F.3d 1279, 1292 (Fed. Cir. 2008).

[3] *Global-Tech Appliances, Inc. v. SEB S.A.*, 563 U.S. 754, 765–66 (2011).

[4] *See Global-Tech Appliances, Inc. v. SEB S.A.*, 563 U.S. 754 (2011).

[5] *See* 35 U.S.C.A. § 271(b).

affirmative intent to cause direct infringement."[6] Thus, "inducement requires evidence of culpable conduct, directed to encouraging another's infringement, not merely that the inducer had knowledge of the direct infringer's activities."[7] A claim of inducement, however, cannot be premised on an omission to act because "active inducement of infringement requires the commission of an affirmative act."[8]

In *MGM Studios, Inc. v. Grokster, Ltd.*,[9] the Supreme Court, relying on patent law, held in a digital copyright case that "one who distributes a device with the object of promoting its use to infringe . . . , as shown by clear expression or other affirmative steps taken to foster infringement, is liable for the resulting acts of infringement by third parties."[10] Liability is based on "purposeful, culpable expression and conduct," and will not be found "on the basis of presuming or imputing fault, but from inferring a patently illegal objective from *statements* and *actions* showing what that objective was."[11] *Grokster* was later characterized by the U.S. Supreme Court as a case involving actual knowledge, rather than merely willful blindness. The Court explained that the defendants in that case "were fully aware—in the ordinary sense of the term—that their file sharing software was routinely used in carrying out the acts that constituted infringement (the unauthorized sharing of copyrighted works) and that these acts violated the rights of copyright holders."[12]

---

[6]*DSU Medical Corp. v. JMS Co.*, 471 F.3d 1293, 1306 (Fed. Cir. 2006) (*en banc*).

[7]*DSU Medical Corp. v. JMS Co.*, 471 F.3d 1293, 1306 (Fed. Cir. 2006) (resolving an apparent conflict between *Hewlett-Packard Co. v. Bausch & Lomb Inc.*, 909 F.2d 1464 (Fed. Cir. 1990) and *Manville Sales Corp. v. Paramount Systems, Inc.*, 917 F.2d 544, 554 (Fed. Cir. 1990)).

[8]*Beverly Hills Fan Co. v. Royal Sovereign Corp.*, 21 F.3d 1558, 1569 (Fed. Cir. 1994).

[9]*Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd.*, 545 U.S. 913 (2005).

[10]*Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd.*, 545 U.S. 913, 937–38 (2005).

[11]545 U.S. at 936–37, 941 (emphasis added); *see generally supra* §§ 4.11[1][E] (analyzing Grokster in connection with secondary copyright law); 4.10[5], 4.11[1][F] (analyzing Grokster in connection with substantial noninfringing use).

[12]*Global-Tech Appliances, Inc. v. SEB S.A.*, 563 U.S. 754, 768–69 (2011).

The Federal Circuit has applied *Grokster* in patent cases.[13]

In *Global-Tech Appliances, Inc. v. SEB S.A.*,[14] the U.S. Supreme Court clarified that inducement liability may be premised on willful blindness, in addition to actual knowledge that the induced acts constitute patent infringement, but mere generalized knowledge of the risk of infringement based on negligence, or even recklessness[15] (or "deliberate indifference to a known risk that a patent exists")[16] is not the appropriate standard for proving inducement under section 271(b). *SEB* was a case where the defendant had purchased and copied an SEB fryer that had been made for sale in a foreign market and therefore lacked U.S. patent markings. It copied everything but the cosmetic features of the fryer and then retained an attorney to conduct a right-to-use study without telling the lawyer that it had copied the fryer from SEB. The attorney did not locate SEB's patent and issued an opinion letter of non-infringement. SEB proceeded to sell the fryer to companies that sold it in the U.S. market and continued to do so even after one of its distributors, Sunbeam, was sued for patent infringement.

In affirming a jury finding of inducement, the U.S. Supreme Court rejected arguments that liability for inducement could be imposed based on either reckless indifference or the fact that a defendant "knew or should have known" about infringing activity. Justice Kennedy, in dissent, wrote

---

[13]*See, e.g., DSU Medical Corp. v. JMS Co.*, 471 F.3d 1293, 1306 (Fed. Cir. 2006) (*en banc*) (clarifying that the Manville standard for intent is valid in light of Grokster and holding that it was reasonable for a jury to conclude that the defendant had no intent to infringe where the evidence, consisting of a legal opinion letter that the product did not infringe and testimony that the defendant did not intend to infringe, supported that conclusion); *see also Golden Blount, Inc. v. Robert H. Peterson Co.*, 438 F.3d 1354, 1365 n.4 (Fed. Cir. 2006) (finding inducement under Grokster based on evidence that defendant had notice of the patent, sold potentially infringing kits, and actively encouraged infringement by including instructions that directed customers to assemble kits in infringing configuration); *MEMC Electronic Materials, Inc. v. Mitsubishi Materials Silicon Corp.*, 420 F.3d 1369, 1379 (Fed. Cir. 2005) (quoting *Grokster* and stating that " '[e]vidence of active steps taken to encourage direct infringement, such as advertising an infringing use or instructing how to engage in an infringing use, show an affirmative intent that the product be used to infringe' ").

[14]*Global-Tech Appliances, Inc. v. SEB S.A.*, 563 U.S. 754 (2011)

[15]*Global-Tech Appliances, Inc. v. SEB S.A.*, 563 U.S. 754, 769-70 (2011).

[16]*Global-Tech Appliances, Inc. v. SEB S.A.*, 563 U.S. 754, 766 (2011).

that willful blindness is not the same as *knowledge,* which is what the Patent Act requires to be shown to establish inducement, "and judges should not broaden a legislative proscription by analogy."[17]

To establish inducement based on willful blindness, Justice Alito wrote that a defendant must: (1) subjectively believe that there is a high probability that a fact exists; and (2) take deliberate actions to avoid learning of that fact. A willfully blind defendant, Justice Alito explained, "is one who takes deliberate actions to avoid confirming a high probability of wrongdoing and who can almost be said to have actually known the critical facts."[18]

To prove inducement, a plaintiff also must show that the defendant took an active step towards encouraging infringement beyond mere knowledge that an allegedly infringing product may be sold. Relying on dictionary definitions, the Supreme Court has explained that *induce* means "[t]o lead on; to influence; to prevail on; to move by persuasion or influence."[19] The addition of the adverb *actively,* in turn, "suggests that the inducement must involve the taking of affirmative steps to bring about the desired result . . . ."[20] For example, in one case pre-dating *SEB* active inducement was shown where the defendant instructed buyers of the product how to use it in an infringing manner.[21] In another case, whether defendants' email communications with a supplier represented product support enabling the purchase of the accused products, and therefore evidence of inducement, was held to present a jury question precluding summary judgment.[22]

Ultimately, the line between actual knowledge and willful

---

[17]*Global-Tech Appliances, Inc. v. SEB S.A.*, 563 U.S. 754, 772 (2011) (Kennedy, J., dissenting).

[18]*Global-Tech Appliances, Inc. v. SEB S.A.*, 563 U.S. 754, 769 (2011).

[19]*Global-Tech Appliances, Inc. v. SEB S.A.*, 563 U.S. 754, 760 (2011), *quoting* Webster's New International Dictionary 1269 (2d ed. 1945).

[20]*Global-Tech Appliances, Inc. v. SEB S.A.*, 563 U.S. 754, 760 (2011).

[21]*Golden Blount, Inc. v. Robert H. Peterson Co.*, 438 F.3d 1354, 1365 (Fed. Cir. 2006).

[22]*MMEC*, 420 F.3d at 1379–80; *see also Metabolite Laboratories, Inc. v. Laboratory Corp. of America Holdings*, 370 F.3d 1354 (Fed. Cir. 2004) (finding inducement based on defendant's publications describing and promoting use of patented method).

blindness may be difficult to draw in some cases.[23]

Inducement, like contributory infringement, requires a showing of an underlying act of infringement.[24]

In the context of an e-commerce platform, the court in *Blazer v. eBay, Inc.*,[25] held that eBay, the online marketplace, was not liable for patent inducement based on either actual knowledge or willful blindness (and also was not liable for either direct or contributory infringement[26]) for items sold by users of its online marketplace even though the plaintiff had provided numerous notice of alleged infringement.

In *Blazer*, eBay, consistent with its policies, did not remove any of the allegedly infringing listings based simply on an assertion of patent infringement, but informed the plaintiff that it would honor a court order if a court agreed that the

---

[23]In *SEB*, the fact that the defendant purchased the patented product outside the United States to avoid U.S. patent markings and did not tell the attorney it retained to provide an opinion letter about the applicable patent was cited as evidence of willful blindness, *see Global-Tech Appliances, Inc. v. SEB S.A.*, 563 U.S. 754, 770–71 (2011), but in Justice Kennedy's view this would also have been circumstantial evidence of knowledge. *See id.* at 774–75 (Kennedy, J., dissenting) (noting that the same "[f]acts that support willful blindness are often probative of actual knowledge.").

The majority's characterization of *Grokster* as a case involving actual knowledge is instructive because in that case the defendants argued that they did not have knowledge of any specific acts of infringement (and the case could have been characterized as involving willful blindness or merely generalized knowledge, coupled with bad intent and affirmative conduct to induce infringement). *See supra* § 4.11[6] (analyzing *Grokster*). In *SEB*, the Court explained that the defendants in Grokster "were fully aware—in the ordinary sense of the term—that their file sharing software was routinely used in carrying out the acts that constituted infringement (the unauthorized sharing of copyrighted works) and that these acts violated the rights of copyright holders." 563 U.S. at 768–69. Thus, specific evidence of knowledge, such as by an admission against interest, is not required. Awareness, "in the ordinary sense of the term" is deemed actual knowledge. In addition, willful blindness—involving at least some level of subjective belief that a fact exists and deliberate actions to avoid learning of the fact—is deemed equivalent to knowledge.

[24]*See Limelight Networks, Inc. v. Akamai Technologies, Inc.*, 134 S. Ct. 2111 (2014) (holding that there can be no liability for induced infringement under 35 U.S.C § 271(b) when there has been no direct infringement under 35 U.S.C § 271(a)).

[25]*Blazer v. eBay, Inc.*, Case No. 1:15-cv-01059-KOB, 2017 WL 1047572 (N.D. Ala. Mar. 20, 2017).

[26]*See supra* §§ 8.10[2][B], 49.03 (addressing contributory infringement and discussing that aspect of the *Blazer* case).

accused products were infringing.[27]

eBay was found not liable for direct infringement because it did not offer for sale or sell the products listed for sale by users of its website.[28] The court explained in *Blazer* that "no reasonable consumer could conclude that by bidding on an eBay listing, he was accepting an offer from eBay itself. eBay's terms of service explicitly advise users that eBay is not making an offer through a listing, and . . . eBay lacks title and possession of the items listed."[29]

With respect to plaintiff's claim for inducement, the court held that merely because eBay had received Notices of Claimed Infringement (NOCI) from the plaintiff did not evidence actual knowledge.[30] As the court explained in distinguishing cases brought between competitors where courts had found a notice letter to be sufficient to create a genuine issue of material fact on knowledge and preclude summary judgment, "eBay does not have expertise in the field of the patent or allegedly infringing products."[31] Because "eBay does not know the art of carpenter bee traps, . . . Mr. Blazer's communications with the company can at most create the inference that eBay knew that Mr. Blazer believed that eBay listings infringed his patent, but they cannot support the inference that eBay itself had actual knowledge of infringement."[32]

Judge Bowdre likewise held that the plaintiff could not establish liability for inducement based on willful blindness, which requires a showing that the defendant (1) had a subjective belief that there was a high probability of infringe-

---

[27]*See Blazer v. eBay, Inc.*, Case No. 1:15-cv-01059-KOB, 2017 WL 1047572, at *6 (N.D. Ala. Mar. 20, 2017).

[28]*Blazer v. eBay, Inc.*, Case No. 1:15-cv-01059-KOB, 2017 WL 1047572, at *2-5 (N.D. Ala. Mar. 20, 2017).

[29]*Blazer v. eBay, Inc.*, Case No. 1:15-cv-01059-KOB, 2017 WL 1047572, at *4 (N.D. Ala. Mar. 20, 2017).

[30]*Blazer v. eBay, Inc.*, Case No. 1:15-cv-01059-KOB, 2017 WL 1047572, at *5 (N.D. Ala. Mar. 20, 2017).

[31]*Blazer v. eBay, Inc.*, Case No. 1:15-cv-01059-KOB, 2017 WL 1047572, at *5 (N.D. Ala. Mar. 20, 2017), *citing Koninklijke Philips NV v. Zoll Med. Corp,* 656 F. App'x 504, 507 (Fed. Cir. 2016) (suit between two manufacturers of external defibrillators); *Fujitsu Ltd. v. Netgear Inc.*, 620 F.3d 1321, 1326 (Fed. Cir. 2010) (suit between competitors in wireless communication technology).

[32]*Blazer v. eBay, Inc.*, Case No. 1:15-cv-01059-KOB, 2017 WL 1047572, at *5 (N.D. Ala. Mar. 20, 2017).

ment, and (2) took deliberate action to avoid obtaining actual knowledge, both of which would need to be shown to establish inducement.[33]

Judge Bowdre explained that to satisfy the requirement for subjective belief of infringement, a defendant must "almost be said to have actually known the critical facts."[34] Likewise, to show deliberate action to avoid obtaining actual knowledge, a plaintiff must show "not merely deliberate indifference but intentional ignorance that surpasses recklessness and negligence."[35] The court held that plaintiff's notices alone were insufficient to support either prong of the test for inducement.

Blazer is analyzed more closely in section 8.10[3].

Inducement may be used as a vehicle to hold corporate officers who actively aid and abet their corporation's infringement personally liable.[36] Liability for inducing patent infringement is based on tort law, and therefore a plaintiff need not pierce the corporate veil to hold officers liable for inducement.[37]

Unlike contributory patent infringement, substantial noninfringing use is not a defense to liability for inducement, which is based on an affirmative intent to infringe.[38]

Patent inducement is analyzed in greater detail in section 8.10[3].

---

[33]*Blazer v. eBay, Inc.*, Case No. 1:15-cv-01059-KOB, 2017 WL 1047572, at *6 (N.D. Ala. Mar. 20, 2017), *citing Global-Tech Appliances, Inc. v. SEB S.A.*, 563 U.S. 754, 769 (2011).

[34]*Blazer v. eBay, Inc.*, Case No. 1:15-cv-01059-KOB, 2017 WL 1047572, at *6 (N.D. Ala. Mar. 20, 2017), *quoting Global-Tech Appliances, Inc. v. SEB S.A.*, 563 U.S. 754, 769-70 (2011).

[35]*Blazer v. eBay, Inc.*, Case No. 1:15-cv-01059-KOB, 2017 WL 1047572, at *6 (N.D. Ala. Mar. 20, 2017), *citing Global-Tech Appliances, Inc. v. SEB S.A.*, 563 U.S. 754, 769 (2011).

[36]*Orthokinetics, Inc. v. Safety Travel Chairs, Inc.*, 806 F.2d 1565, 1579 (Fed. Cir. 1986).

[37]*Orthokinetics, Inc. v. Safety Travel Chairs, Inc.*, 806 F.2d 1565, 1579 (Fed. Cir. 1986).

[38]*Dynacore Holdings Corp. v. U.S. Philips Corp.*, 363 F.3d 1263, 1275–76 n.6 (Fed. Cir. 2004); *see also Grokster*, 545 U.S. at 938 (rejecting it as a defense to a claim of copyright inducement); *supra* §§ 4.10[5], 4.11[7] (analyzing substantial noninfringing use under copyright law).

49.10 Child Pornography and Obscene Content

49.10[1] In General

Unlike mere pornography, which is entitled to First Amendment protection, child pornography and obscene material do not constitute constitutionally protected speech and may be banned.[1] State and federal laws prohibit even the mere possession of child pornography and, while the Supreme Court has recognized a narrow right to possess obscene material in one's home, it may not be distributed or sold and therefore effectively may not be posted or remain online.

Child pornography and obscenity statutes typically contain *scienter* requirements that make it unlikely that ordinary site owners or service providers would be subject to criminal liability based on user content or conduct that they do not know about or condone. Pursuant to the Protection of Children from Sexual Predators Act of 1998, however, site owners and service providers must report child pornography (once reported to them or discovered) to appropriate police agencies in order to avoid significant fines. Although there is no similar requirement with respect to content which is obscene, it is generally advisable to respond to third-party complaints about obscene material. Site owners and service providers generally need not affirmatively search for child pornography or obscene material that otherwise has not been reported or discovered. As a practical matter, however, many do because it can create customer relations issues and create the impression that a company is not compliance-oriented if this type of material remains online.

In addition to legal compliance, site owners and service providers should consider taking steps affirmatively to protect children and others on their networks. Best practices for the safety of minors on social networks is specifically addressed in section 51.09[3] and should be reviewed by sites or services that host user generated content.

49.10[2] Child Pornography Laws and Reporting Requirements

U.S. law prohibits the dissemination, transportation,

[Section 49.10[1]]

[1]*See Bose Corp. v. Consumers Union*, 466 U.S. 485, 504 (1984); *see generally supra* § 39.02[1].

importation and even mere possession of child pornography, which is sexual content that depicts minors.[1] Child pornography statutes generally have been construed to impose criminal liability only in cases where *scienter*, or intent, may be shown.[2] Site owners and service providers should be diligent about responding to complaints about child pornography.

Pursuant to the Protection of Children from Sexual Predators Act of 1998 and implementing regulations, anyone engaged in providing an *electronic communication service*[3] or a *remote computing service*[4] to the public[5] who obtains actual knowledge of an "apparent violation" of child pornography laws must report this information "as soon as reasonably possible" by calling the National Center for Missing and Exploited Children (NCMEC) to obtain an identification number and a password to be able to file a report with NCMEC's Cyber Tipline using NCMEC's online form (www.CyberTipline.com).[6] NCMEC, in turn, is responsible for notifying federal law enforcement agencies.[7] Although the issue rarely comes up, a court in Ohio held that a service provider could not be held liable for a privacy law violation—in this case compliance with the provisions of the Cable

---

[Section 49.10[2]]

[1]*See* 18 U.S.C.A. §§ 2251 *et seq*.; *Osborne v. Ohio*, 495 U.S. 103 (1990) (possession); *New York v. Ferber*, 458 U.S. 747 (1982) (distribution); *see generally supra* § 40.01.

[2]*See U.S. v. X-Citement Video, Inc.*, 513 U.S. 64, 69–71 (1994); *see generally supra* § 40.03.

[3]*An electronic communication service* is given the same meaning as under the Electronic Communications Privacy Act—namely, "any service which provides to users . . . the ability to send or receive wire or electronic communications." *See* 18 U.S.C.A. §§ 2258A(a)(1), 2510; *infra* § 50.06[4][D] (analyzing what type of service constitutes an ECS provider).

[4]A *remote computing service* likewise is given the same meaning as under ECPA. The term thus refers to an entity that provides computer storage or processing services to the public by means of an electronic communications system. *See* 18 U.S.C.A. §§ 2258A(a)(2), 2711; *infra* § 50.06[4][D] (analyzing what type of service constitutes an RCS provider).

[5]These definitions expressly include public networks but likely do not apply to intranets or other purely internal networks, even if such networks are connected to the Internet or are otherwise accessed through means of interstate communications. *See supra* § 44.06 (analyzing ECPA's legislative history).

[6]*See* 18 U.S.C.A. §§ 2258A, 2702(b)(6); 28 C.F.R. §§ 81.11 to 81.13.

[7]28 C.F.R. § 81.13.

Communications Policy Act[8]—for reporting child pornography to law enforcement officials pursuant to section 2258A.[9]

Which type of service constitutes an *electronic communication service* or a *remote computing service* is analyzed extensively in section 50.06[4][D] in the next chapter, but generally has been held to include providers of email,[10] text messaging services,[11] private messaging or email services on social networks such as Facebook and MySpace,[12] microblogs such as Twitter[13] and other interactive sites and services, including mobile providers,[14] but not certain

---

[8]47 U.S.C.A. § 551; *see generally infra* § 50.06[5] (discussing the Act).

[9]*See Jurek v. AT&T*, No. 5:13 CV 1784, 2013 WL 5298347 (N.D. Ohio Sept. 20, 2013).

[10]*E.g., Warshak v. United States*, 532 F.3d 521, 523 (6th Cir. 2008); *Theofel v. Farey-Jones*, 359 F.3d 1066, 1075 (9th Cir.), *cert. denied,* 543 U.S. 813 (2004); *Bower v. Bower*, 808 F. Supp. 2d 348, 350 (D. Mass. 2011) ("courts have repeatedly held that providers such as Yahoo! and Google may not produce emails in response to civil discovery subpoenas"); *In re Subpoena Duces Tecum to AOL, LLC*, 550 F. Supp. 2d 606, 611 (E.D. Va. 2008); *Freedman v. America Online, Inc.*, 325 F. Supp. 2d 638, 644 n.4 (E.D. Va. 2004) (ruling that AOL is an "electronic communication service" provider).

[11]*E.g.*, *Quon v. Arch Wireless Operating Co.*, 529 F.3d 892, 901 (9th Cir. 2008) (holding that the text messaging pager services provided by Arch Wireless constituted an ECS because it enabled the plaintiff and others to "send or receive . . . electronic communications" (text messages)), *rev'd on other grounds sub. nom Ontario v. Quon*, 560 U.S. 746 (2010); *Mintz v. Mark Bartelstein & Associates, Inc.*, 885 F. Supp. 2d 987, 991 (C.D. Cal. 2012) (holding that AT&T was an ECS with respect to the text messages at issue in that case); *Flagg v. City of Detroit*, 252 F.R.D. 346, 362–63 (E.D. Mich. 2008) (holding SkyTel to be an ECS provider of text messages).

[12]*See, e.g.*, *Crispin v. Christian Audigier, Inc.*, 717 F. Supp. 2d 965, 980 (C.D. Cal. 2010) (stating that social networking sites Facebook and MySpace that provide private messaging or email services qualify as electronic communication services).

[13]*See, e.g., In re Application of the U.S. for an Order Pursuant to 18 U.S.C. § 2703(d)*, 830 F. Supp. 2d 114, 118 (E.D. Va. 2011) ("Twitter is a social networking service that permits users to post pithy messages using short communications called 'tweets,' and to read the tweets of other users . . . In addition to posting their own tweets, users may send messages to a single user ('direct messages') or repost other users' tweets ('retweet').").

[14]*E.g.*, *In re Application of U.S. for an Order for Prospective Cell Site Location Information on a Certain Cellular Telephone*, 460 F. Supp. 2d 448, 459 (S.D.N.Y. 2006); *In re Application for a Court Order Authorizing AT&T to Provide Historical Cell Tower Records,* No. ST–11–WS–08, ST–11–WS–09, ST–11–WS–10, ST–11–WS–12, 2011 WL 7092589, at *3

e-commerce sites such as websites that sold airline tickets.[15] An extensive analysis of the statutory terms, legislative history and case law is set forth in section 50.06[4][D].

A provider who knowingly and willfully fails to make a required report may be fined up to $150,000 (or $300,000 for subsequent violations).[16] The statute makes clear, however, that providers are not required to monitor users, customers or subscribers or their communications.[17]

49.10[3] Obscene Content

Obscene material effectively may not be posted, stored, or transmitted over the Internet. U.S. law prohibits the sale, distribution or importation of obscene content.[1] In the 1960s, the U.S. Supreme Court recognized a narrow right to possess obscene material in the privacy of one's home.[2] Since that time, however, the Court has clarified that this limited right does not create "a correlative right to receive it, transport it, or distribute it" in interstate commerce, even for private use, or create a zone of privacy when the person takes such content beyond her front door.[3] Accordingly, obscene content may not be posted, transmitted or stored online. Since obscenity is judged by local community stan-

---

(V.I. Super. Apr. 29, 2011).

[15]*See, e.g., In re Jetblue Airways Corp. Privacy Litigation*, 379 F. Supp. 2d 299, 308–09 (E.D.N.Y. 2005) (holding that the airline was not an ECS provider where it simply sold its products online, but did not provide Internet access; JetBlue was a provider of air travel services and consumer of electronic communication services); *Dyer v. Northwest Airlines Corp.*, 334 F. Supp. 2d 1196, 1199 (D.N.D. 2004) ("Courts have concluded that 'electronic communication service' encompasses internet service providers as well as telecommunications companies whose lines carry internet traffic, but does not encompass businesses selling traditional products or services online."); *see generally infra* § 50.06[4][D] (providing additional examples and analyzing the issue more extensively).

[16]*See* 18 U.S.C.A. § 2258A(e).

[17]*See* 18 U.S.C.A. § 2258A(f).

[Section 49.10[3]]

[1]*See* 18 U.S.C.A. §§ 1462, 1465; *see generally supra* § 40.02.

[2]*See Stanley v. Georgia*, 394 U.S. 557 (1969).

[3]*See U.S. v. Orito*, 413 U.S. 139, 141–42 (1973); *U.S. v. Thomas*, 74 F.3d 701, 710 (6th Cir.), *cert. denied*, 519 U.S. 820 (1996); *see generally supra* § 40.02.

dards,[4] this means that site owners and service providers should assess material based on the standards of the most conservative jurisdiction in the United States.[5]

Site owners and service providers need not affirmatively report obscene content but should immediately remove it from their servers or disable links to it. Obscenity laws generally prohibit knowing conduct. While U.S. law does not impose a duty on providers to affirmatively search out content, providers who receive notice that obscene material is on their servers and fail to take action theoretically could expose themselves to prosecutions for knowingly distributing it.[6] Businesses therefore should adopt policies and/or procedures for responding to such complaints.

The criminal provisions of the Communications Decency Act,[7] which were judicially limited to apply only to obscene communications directed to minors,[8] include specific exemptions potentially applicable to mere access providers or employers that could provide useful guidance on best practices for some types of services.[9] As a practical matter, however, pre-existing obscenity laws provide broader coverage without the limitations of the CDA,[10] making it unlikely that the government would ever charge criminal conduct under this statute (or that access providers or employers could avoid any liability by complying with its terms).

---

[4]*See, e.g., Miller v. California*, 413 U.S. 15, 24 (1973); *see also U.S. v. Thomas*, 74 F.3d 701 (6th Cir.) (rejecting the argument that "contemporary community standards" in an Internet obscenity case should be evaluated by the mores of cyberspace, rather than the local community on *terra firma* where the prosecution was brought), *cert. denied*, 519 U.S. 820 (1996); *see generally supra* § 40.02.

[5]Federal obscenity statutes contain especially broad venue provisions which have been construed to authorize a criminal prosecution in any district "from, through, or into which the allegedly obscene material moves." *U.S. v. Thomas*, 74 F.3d 701 (6th Cir.), *cert. denied*, 519 U.S. 820 (1996); *see also* 18 U.S.C.A. § 3237.

[6]Once posted on a publicly accessible site, material is effectively distributed to the public.

[7]47 U.S.C.A. § 223.

[8]*See Reno v. American Civil Liberties Union*, 521 U.S. 844 (1997); *see generally supra* § 41.02.

[9]*See supra* §§ 41.02, 49.03.

[10]*See generally supra* § 41.02.

49.10[4] Material Deemed Harmful to Minors

Congress has sought unsuccessfully to regulate material online that is deemed harmful to minors. While site owners and service providers face no liability under federal law for allowing material harmful to minors, state attorneys general may take action to protect children. Many sites and services may also find it to be a good business practice to be seen as protecting children online.

The leading case defining the extent to which the government may regulate speech directed at minors is *Ginsberg v. New York*.[1] In that case, the Supreme Court upheld the constitutionality of a New York statute that prohibited vendors from selling pornographic material to children that—although not obscene by adult standards—was deemed obscene as to children, in part because adults could otherwise gain access to such material. The Court in *Ginsberg* held that material is obscene as to minors if it is: (1) "patently offensive to prevailing standards in the adult community as a whole with respect to what is suitable . . . for minors"; (2) appeals to the prurient interest of minors; and (3) is "utterly without redeeming social importance to minors."[2]

In the Communications Decency Act,[3] Congress unsuccessfully sought to extend *Ginsberg* to cyberspace, in a somewhat inartfully drafted statute that purported to prohibit "indecent" and "patently offensive" communications to minors. In striking down most aspects of the CDA, the U.S. Supreme Court, in *Reno v. ACLU*,[4] recognized sweeping First Amendment rights in cyberspace, significantly limiting the ability of legislators to enact even more narrowly tailored statutes modeled on *Ginsberg* to protect children online. The Court also arguably limited legislators' ability to enact zoning regulations such as the one upheld in *Renton v. Playtime Theatres, Inc.*,[5] to restrict non-obscene adult material to particular areas in cyberspace that would be inaccessible to children. The Court, however, left open the possibility for

---

[Section 49.10[4]]

[1] *Ginsberg v. New York*, 390 U.S. 629 (1968).

[2] *Ginsberg v. New York*, 390 U.S. 629, 633 (1968).

[3] The relevant provisions previously were codified at 47 U.S.C.A. § 223.

[4] *Reno v. American Civil Liberties Union*, 521 U.S. 844 (1997).

[5] *City of Renton v. Playtime Theatres, Inc.*, 475 U.S. 41 (1986).

regulation in the future, if new technologies emerge that allow for more effective cyberzoning.[6]

Congress thereafter enacted the Child Online Protection Act (COPA),[7] which addressed the specific infirmities identified by the Court in *Reno v. ACLU*[8] and more narrowly targeted commercial websites that made available material harmful to minors, which were required to implement age verification mechanisms to avoid liability. Although the Supreme Court initially upheld the statute in response to a facial challenge in *Ashcroft v. ACLU*,[9] two years later it affirmed a lower court order preliminarily enjoining COPA's enforcement. In the second *Ashcroft v. ACLU*[10] decision, a majority of the Court found the government unlikely to meet its burden of proving that there were no less restrictive alternatives to the age verification requirements imposed on commercial pornography sites to prevent children from accessing these locations, underscoring that it is difficult if not impossible for Congress to restrict access to minors to online material deemed harmful to minors. Unlike in the physical world, children's access to material obscene as to minors may not easily be blocked without also impacting adult access to this same material, which for adults potentially may be constitutionally protected. For better or worse, courts, in balancing these rights, have weighed in favor of protecting the rights of adults to unrestricted access to material obscene as to children, rather than the interest of the government in protecting children from gaining access to this material.[11]

49.10[5] Civil Liability

Courts generally have not been receptive venues for efforts to hold Internet sites and services liable for misconduct by their users, including physical and sexual attacks that occur in the physical world by people who first made contact

---

[6] *See supra* § 41.02.

[7] 47 U.S.C.A. § 231; *see supra* § 41.03.

[8] *Reno v. American Civil Liberties Union*, 521 U.S. 844 (1997); *see generally supra* § 41.02.

[9] *Ashcroft v. American Civil Liberties Union*, 535 U.S. 564 (2002).

[10] *Ashcroft v. American Civil Liberties Union*, 542 U.S. 656 (2004); *see generally supra* § 41.03.

[11] *See supra* §§ 41.02 to 41.04.

online. The Communications Decency Act,[1] which is analyzed extensively in section 37.05, insulates interactive computer service providers and users from liability premised on holding a site or service liable as a speaker or publisher of third party material. Courts have construed the CDA broadly to preempt suits for user misconduct involving child safety, among other things, where liability against an interactive computer service provider or user, however characterized or framed, ultimately is premised on publication of third party content (such as social network profiles or communications in chat rooms). Thus, for example, courts have held that the CDA preempts claims by parents against Internet sites and services where children have met adults who then allegedly abused them,[2] and by the victim of a sex trafficker against the publisher of online classified ads as a result of which the plaintiff allegedly was victimized.[3] It has also been held to preempt claims by a tort victim against the Internet service where the plaintiff's assailant had allegedly purchased the gun used against him,[4] against a social network for failing to

---

[Section 49.10[5]]

[1]47 U.S.C.A. § 230(c).

[2]*See, e.g.*, *Doe v. MySpace, Inc.*, 528 F.3d 413 (5th Cir.), *cert. denied*, 555 U.S. 1031 (2008); *Doe IX v. MySpace, Inc.*, 629 F. Supp. 2d 663 (E.D. Tex. 2009); *Doe II v. MySpace, Inc.*, 175 Cal. App. 4th 561, 96 Cal. Rptr. 3d 148 (Cal. App. 2009); *Doe v. America Online, Inc.*, 783 So. 2d 1010 (Fla. 2001).

In *Doe v. SexSearch.com*, 502 F. Supp. 2d 719 (N.D. Ohio 2007), *aff'd on other grounds*, 551 F.3d 412 (6th Cir. 2008), the district court had held that the CDA preempted the common law tort and contract claims brought by an anonymous user of an "adult" dating service based on the service's failure to prevent minors from joining, but the Sixth Circuit ultimately affirmed the court's dismissal based on SexSearch's Terms and Conditions, without reaching the issue of the CDA's applicability. *See supra* § 37.05[6] (discussing the case in connection with social network liability).

[3]*See, e.g.*, *Doe No. 1 v. Backpage.com, LLC*, 817 F.3d 12, 18-24 (1st Cir. 2016) (affirming dismissal of claims for civil remedies under the Trafficking Victims Protection Reauthorization Act, 18 U.S.C.A. § 1595, as preempted by 47 U.S.C.A. § 230(c)(1), in an opinion that was abrogated with respect to the federal trafficking claim, by the subsequent enactment of 47 U.S.C.A. § 230(e)(5)); *M.A. v. Village Voice Media Holdings LLC*, 809 F. Supp. 2d 1041 (E.D. Mo. 2011); *see generally supra* § 37.05 (analyzing this issue and discussing additional cases).

[4]*See Gibson v. Craigslist, Inc.,* No. 08 Civ. 7735 (RMB), 2009 WL 1704355 (S.D.N.Y. June 15, 2009) (granting a motion to dismiss).

promptly remove a profile that allegedly led to violence,[5] and for failing to act to prevent statements made in a chatroom or transmission of a computer virus,[6] among other claims.[7] The Ninth Circuit, however, has carved out a narrow exception where an interactive computer service fails to warn about a hazard, where it has actual knowledge of the hazard that it learned offline.[8] The scope of CDA preemption is analyzed exhaustively in section 37.05.

Service providers also may be able to benefit from the exemption provided for in the Child Online Protection Act for restricting or preventing the transmission of, or access to, a communication obscene as to minors.[9]

49.11 Advertising (including Spamming and Viral Marketing)

Site owners and service providers potentially may be held secondarily liable for advertisements that appear on their sites that infringe intellectual property laws, primarily under theories of secondary copyright, trademark and right of publicity laws.[1] Advertisements may be posted on a blog or other website or distributed by email. Advertisements also may appear as sponsored links or banner advertisements on a site.[2] As discussed earlier in this chapter, site owners and service providers may limit their liability for infringing

---

[5]*See Klayman v. Zuckerberg*, 753 F.3d 1354 (D.C. Cir. 2014) (holding negligence and intentional assault claims against Facebook and its founder preempted by the CDA because neither defendant created nor provided the Third Palestinian Intifada Facebook page at issue in the suit, which allegedly promoted religious hate and violence).

[6]*See Green v. America Online (AOL)*, 318 F.3d 465 (3d Cir.) (chatroom statements and the alleged transmission of a virus), *cert. denied*, 540 U.S. 877 (2003).

[7]*See supra* §§ 37.05[1][C], 37.05[3][B][ii].

[8]*See Doe No. 14 v. Internet Brands, Inc.*, 824 F.3d 846 (9th Cir. 2016) (holding that the CDA did not bar a claim against the social networking site for models, Model Mayhem, based on the site's failure to warn the plaintiff, a user of the site, of prior attacks on users by the two men who contacted her for an audition and then raped her, where the alleged duty arose based on information learned offline); *see generally supra* § 37.05[3][B][ii] (analyzing *Doe No. 14*).

[9]*See* 47 U.S.C.A. § 231(c)(2); *see supra* § 49.10[4]. This provision of COPA was not enjoined. *See supra* § 41.02.

[Section 49.11]

[1]*See supra* §§ 49.05, 49.06, 49.07.

[2]*See supra* § 9.11 (keywords, banner advertisements and sponsored

content by complying with the DMCA,[3] pursuant to the innocent printer's and publisher's defense and the defense for fair use comparative advertising,[4] and by responding to take down notices for publicity violations.[5]

Where advertisements are sent by email, secondary liability may be imposed for violations of the CAN-SPAM Act, generally based on knowledge or conscious avoidance of knowledge. Secondary liability under the CAN-SPAM Act is addressed generally in section 29.03[6] and in connection with affiliate marketing in section 29.03[8].

Similarly, where advertisements are sent via text messaging, vicarious liability may be imposed for violations of the Telephone Consumer Protection Act ("TCPA")[6] but only to the extent that the conduct of an employee or agent or third-party telemarketer acting within the scope of authority may be attributed to a company.[7] Liability for text messages under the TCPA is analyzed in section 29.16.

49.12 Cable Communications Policy Act

The Cable Communications Policy Act provides that "[n]o person shall intercept or receive or assist in intercepting or receiving any communications service offered over a cable

---

links).

[3] *See supra* § 49.05.

[4] *See supra* § 49.06.

[5] *See supra* § 49.07.

[6] 47 U.S.C.A. § 227.

[7] *See, e.g.*, *In re: Jiffy Lube Int'l, Inc. Text Spam Litig.*, 847 F. Supp. 2d 1253, 1257 (S.D. Cal. 2012) (holding that the plaintiff had stated a claim for vicarious liability under section 227(b)(1)(A) where the defendant hired the entity that sent the text message at issue in the case); *Hickey v. Voxernet LLC*, 887 F. Supp. 2d 1125, 1129 (W.D. Wash. 2012) (holding that a defendant may be liable for the transmission of messages that it did not physically send where the defendant "controlled sending the message."); *Accounting Outsourcing LLC v. Verizon Wireless Personal Communications, L.P.*, 329 F. Supp. 2d 789, 806 (M.D. La. 2004) (holding that TCPA liability could extend to advertisers hired to send unsolicited messages and holding that "congressional tort actions . . . implicitly include the doctrine of vicarious liability, whereby employers are liable for the acts of their agents and employees."), *citing Meyer v. Holley*, 357 U.S. 280, 285 (2003).

system, unless specifically authorized . . .” to do so.[1] The Act further provides that “[n]o person not being authorized by the sender shall intercept any radio communication and divulge or publish . . .” it and that “[n]o person not being entitled thereto shall receive or assist in receiving any interstate or foreign communications by radio . . . .”[2] These provisions largely are used to target the theft of cable and satellite transmissions through the use of “black boxes” and other unauthorized converters which permit reception of cable services without paying for them.[3] The statutes also have been used to sue bar or motel owners for providing access to patrons beyond the scope of their authorized use.[4] While the issue has rarely been litigated, in *Zuffa, LLC v. Justin.TV, Inc.,*[5] a district court in Nevada held that a sports promotion company could not maintain a claim under the Act against a UGC site based on one of its users having provided access to live streaming of plaintiff's mixed martial arts fight via the site. The court held that the plaintiff could not state a claim because Justin.tv, a live streaming UGC site, had no relationship with the original cable or satellite signal and therefore did not *receive* or *intercept* the transmission rebroadcast by its user.[6] The court noted in *dicta* that were it to allow such a claim for user conduct “it would have to allow similar Communications Act claims against scores of ‘cloud computing’ service providers . . . .”[7]

If such a claim could be asserted, the service provider likely would be able to avail itself of the safe harbor created by the Good Samaritan exemption created by the Telecommunications Act of 1996 (colloquially referred to as the

---

[Section 49.12]

[1]47 U.S.C.A. § 553(a)(1).

[2]47 U.S.C.A. § 553(a)(1).

[3]*See* H.R. Rep. No. 98-934, *reprinted in* 1984 U.S.C.C.A.N. 4655, 4721.

[4]*See Zuffa, LLC v. Justin.TV, Inc.*, 838 F. Supp. 2d 1102, 1106 (D. Nev. 2012) (summarizing cases).

[5]*Zuffa, LLC v. Justin.TV, Inc.*, 838 F. Supp. 2d 1102 (D. Nev. 2012).

[6]*See Zuffa, LLC v. Justin.TV, Inc.*, 838 F. Supp. 2d 1102, 1107 (D. Nev. 2012).

[7]*Zuffa, LLC v. Justin.TV, Inc.*, 838 F. Supp. 2d 1102, 1107 n.6 (D. Nev. 2012).

CDA),[8] to the extent liability was premised on retransmitting (*publishing* or *speaking*) user-submitted content.[9]

49.13 Other Illegal Acts

Site owners and service providers potentially could be held liable for other illegal acts that occur on their sites. To the extent not covered by the Good Samaritan exemption,[1] potentially illegal acts by users should be prohibited in service contracts,[2] Terms of Use[3] and to compel customers, subscribers and other users to comply with the law (or discontinue service to them if they do not).

49.14 False Advertising Exposure for Publicizing User Generated Content

Even where a site or service may not be held secondarily liable for trademark or copyright infringement, there is some small risk that it could be sued for false advertising to the extent it publicizes the availability of user generated content that ultimately turns out to be infringing. While false advertising claims arising under state law may be preempted by the Good Samaritan exemption,[1] claims under the Lanham Act are excluded from CDA preemption. Most users, however, cannot bring false advertising claims against sites and services under the Lanham Act. To have standing to bring a claim, a plaintiff must allege (1) an injury to a commercial interest in reputation or sales; and (2) economic or reputational injury flowing directly from the deception wrought by the defendant's advertising (which occurs when the deception of consumers causes them to withhold trade

---

[8] 47 U.S.C.A. § 230(c).

[9] *See supra* § 49.04; *see generally supra* § 37.05 (analyzing the provision in greater detail).

[Section 49.13]

[1] 47 U.S.C.A. § 230(c); *supra* § 49.10[5] (discussing claims of user misconduct preempted by the CDA); *see generally supra* § 37.05 (analyzing the provision in substantially greater detail).

[2] *See supra* chapter 23.

[3] *See supra* chapter 22; see *also supra* §§ 21.03, 21.04 (online contract formation).

[Section 49.14]

[1] 47 U.S.C.A. § 230(c); *supra* § 49.04.

from the plaintiff).[2] Rights owners, competitors and others, however, may have standing to sue.

In *Tiffany (NJ) Inc. v. eBay, Inc.*,[3] the Second Circuit remanded the case on the narrow question of whether extrinsic evidence suggested that sponsored link advertisements were misleading or confusing "insofar as they implied the genuineness of Tiffany goods on eBay's site[,]" based on eBay's generalized knowledge that in addition to genuine Tiffany products, counterfeit items were available on eBay.[4] In that case, the court had otherwise affirmed judgment for eBay on Tiffany's claim for contributory liability under the Lanham Act based on user listings for allegedly counterfeit goods,[5] but explained that the fact that eBay did not have knowledge that specific listings were for counterfeit goods, while relevant to contributory infringement, "sheds little light on whether the advertisements were misleading insofar as they implied the genuineness of Tiffany goods on eBay's site."[6] It further explained:

> It is true that eBay did not itself sell counterfeit Tiffany goods; only the fraudulent vendors did, and that is in part why we conclude that eBay did not infringe Tiffany's mark. But eBay did affirmatively advertise the goods sold through its site as Tiffany merchandise. The law requires us to hold eBay accountable for the words that it chose insofar as they misled or confused consumers.[7]

In so ruling, the court dismissed concerns raised by *amici* that a site that hosts user content could not advertise without risking liability, but the court concluded that a "disclaimer might suffice."[8]

In remanding the case, Second Circuit did not suggest that eBay *in fact* would be held liable; merely that the

---

[2]*Lexmark Int'l, Inc. v. Static Control Components, Inc.*, 134 S. Ct. 1377 (2014); *see generally supra* § 6.12[5].

[3]*Tiffany (NJ) Inc. v. eBay Inc.*, 600 F.3d 93 (2d Cir.), *cert. denied*, 562 U.S. 1082 (2010).

[4]*Tiffany (NJ) Inc. v. eBay Inc.*, 600 F.3d 93, 113–14 (2d Cir.), *cert. denied*, 562 U.S. 1082 (2010).

[5]*See supra* § 49.06.

[6]*Tiffany (NJ) Inc. v. eBay Inc.*, 600 F.3d 93, 114 (2d Cir.), *cert. denied*, 562 U.S. 1082 (2010).

[7]*Tiffany (NJ) Inc. v. eBay Inc.*, 600 F.3d 93, 113 (2d Cir.), *cert. denied*, 562 U.S. 1082 (2010).

[8]*Tiffany (NJ) Inc. v. eBay Inc.*, 600 F.3d 93, 113 (2d Cir.), *cert. denied,* 562 U.S. 1082 (2010).

district court erred in not considering potential extrinsic evidence.

On remand, the district court entered judgment for eBay, finding that the evidence did not support a finding of false advertising because Tiffany could not show that the advertisements in fact were misleading or confusing to consumers.[9]

While *Tiffany v. eBay* underscores that it would be extremely difficult to hold a legitimate site or service liable for publicizing user listings or content, the Second Circuit's opinion also serves as a cautionary warning about potential exposure that could arise and suggests that care should be taken about the way user content is promoted.

49.15 Liability Exemptions for Monitoring and Disclosures Under the Cybersecurity Information Sharing Act (CISA)

The Cybersecurity Information Sharing Act (CISA)[1] authorizes companies to take certain defensive measures on their own information systems to protect against security threats, and encourages companies to voluntarily share information with each other and with federal, state, local and tribal governments, to aid in combatting cyberattacks. Although the statute creates incentives for compliance—including exemptions from liability for monitoring information systems or sharing or receiving cyber threat indicators—participation by private entities is voluntary. The statute, including its liability exemptions, is analyzed in section 27.04[1.5].

---

[9] *See Tiffany (NJ) Inc. v. eBay, Inc.*, Case No. 04 Civ. 4607 (RJS), 2010 WL 2722894 (S.D.N.Y. Sept. 13, 2010) (entering judgment for eBay on Tiffany's false advertising claim following remand). Tiffany had presented the following evidence: (1) declarations from three eBay customers who believed that they had bought counterfeit Tiffany goods on eBay; (2) testimony from a Tiffany employee that Tiffany had received numerous emails complaining of counterfeit Tiffany goods on eBay; and (3) 125 emails sent by customers to eBay complaining of Tiffany goods. The court noted in passing that this limited evidence was "deficient . . . to show the effect of the advertisements on consumers in general . . . ," but held specifically that it was insufficient because it did not establish that "any consumer was misled by eBay's advertisements." *Id*. at *2 (noting additional defects with the specific declarations submitted).

[Section 49.15]

[1] 6 U.S.C.A. §§ 1501 to 1510.

49.16 Cloud Act Liability Exemptions

The Clarifying Lawful Overseas Use of Data Act (CLOUD Act), which was signed into law in 2018, was intended to make clear that data stored in the Cloud by U.S. entities in foreign countries was subject to U.S. warrants and court orders. The statute was enacted in the face of a pending U.S. Supreme Court case that raised the issue of the potentially limited reach of ECPA internationally, following a ruling by the Second Circuit, holding that the Stored Communications Act did not authorize a U.S. court to compel a U.S.-based service provider to disclose the contents of a customer's electronic communications stored on servers located outside the United States.[1] Because of the risk that compliance with a U.S. court order, for data stored overseas, could place a service provider under conflicting obligations under U.S. and local law, the CLOUD Act creates a mechanism for both service providers and governments to address the issue and affords a liability exemption for service providers under certain circumstances.

The CLOUD Act amended the Electronic Communications Privacy Act (ECPA) to clarify that ECPA applies regardless of whether a communication, record, or other information is located within or outside the United States. Pursuant to the statute, electronic communication service (ECS) and remote computing service (RCS) providers generally are obligated to comply with the terms of ECPA regardless of whether a communication, record, or other information is located within or outside of the United States.[2] The CLOUD Act provides that an ECS or RCS provider "shall comply with the obligations" imposed by ECPA "to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control,

---

[Section 49.16]

[1]*See In re A Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.*, 829 F.3d 197, 222 (2d Cir. 2016) ("We conclude that Congress did not intend the SCA's warrant provisions to apply extraterritorially. The focus of those provisions is protection of a user's privacy interests. Accordingly, the SCA does not authorize a U.S. court to issue and enforce an SCA warrant against a United States-based service provider for the contents of a customer's electronic communications stored on servers located outside the United States."), *vacated as moot sub. nom U.S. v. Microsoft,* 138 S. Ct. 1186 (2018).

[2]*See* 18 U.S.C.A. § 2713.

regardless of whether such communication, record, or other information is located within or outside of the United States."[3] The CLOUD Act, however, includes a mechanism for an ECS or RCS provider—or a foreign ECS or RCS provider—to seek a motion to quash or modify legal process where the provider reasonably believes (1) that the customer or subscriber is not a U.S. person and does not reside in the United States, and (2) the required disclosure would "create a material risk" that the provider would violate the laws of a qualifying foreign government.[4]

The CLOUD Act also created an exemption for service providers. The statute provides that no cause of action may be brought against an ECS or RCS provider (or their officers, employees, agents, or other specified persons) for providing information, facilities, or assistance in accordance with a court order issued pursuant to ECPA, a request for emergency pen register and trap and trace device installation,[5] or an order from a foreign government that is subject to an executive agreement.[6] The Act also establishes a defense for good faith reliance on certain court orders, including a good faith belief that the conduct complained of was permitted by an order of certain foreign governments.[7]

The CLOUD Act, and its interplay with ECPA, is analyzed

---

[3]18 U.S.C.A. § 2713.

[4]18 U.S.C.A. § 2703(h)(2). A *qualifying foreign government* is defined as a foreign government with which the United States has an executive agreement that has entered into force pursuant to 18 U.S.C.A. § 2523, and the laws of which provide to ECS and RCS providers "substantive and procedural opportunities similar to those provided" under sections 2703(h)(2) (providing for a motion to quash) and 2703(h)(5) (creating a safe harbor for disclosures to qualifying foreign governments). *See* 18 U.S.C.A. § 2703(h)(1)(A). A service provider is required to preserve, but not obligated to produce, information sought during the pendency of a motion, unless the court finds that immediate production is necessary to prevent an adverse result (as identified in section 2705(a)(2)). *See* 18 U.S.C.A. § 2703(h)(4).

In Europe, the European Union's General Data Protection Regulation (GDPR) may impose restrictions on the disclosure of information pursuant to U.S. court orders. Under EU law, international data transfers pursuant to court orders must be based on an international agreement, such as a Mutual Legal Assistance Treaty (MLAT). *See generally supra* § 26.04 (addressing the GDPR).

[5]*See* 18 U.S.C.A. § 3125.

[6]18 U.S.C.A. § 3124(d).

[7]*See* 18 U.S.C.A. § 3124(e).

more extensively in section 50.06[4].

E-COMMERCE & INTERNET LAW: TREATISE WITH FORMS 2D 2019

Ian C. Ballon

NEW AND IMPORTANT FEATURES FOR 2019 NOT FOUND ELSEWHERE

The Preeminent Internet and Mobile Law Treatise from a leading Internet litigator — now a 5 volume set!

To order call **1-888-728-7677**
or visit **legalsolutions.thomsonreuters.com**

Key Features of E-Commerce & Internet Law

- The California Consumer Privacy Act, GDPR, California IoT security statute, Vermont data broker registration law, Ohio safe harbor statute and other important privacy and cybersecurity laws
- Understanding conflicting law on mobile contract formation, unconscionability and enforcement of arbitration and class action waiver clauses
- The most comprehensive analysis of the TCPA's application to text messaging and its impact on litigation found anywhere
- Complete analysis of the Cybersecurity Information Sharing Act (CISA), state security breach statutes and regulations, and Defend Trade Secrets Act (DTSA) and their impact on screen scraping and database protection, cybersecurity information sharing and trade secret protection, privacy obligations and the impact that Terms of Use and other internet and mobile contracts may have in limiting the broad exemption from liability otherwise available under CISA
- Comprehensive and comparative analysis of the platform liability of Internet, mobile and cloud site owners, and service providers, for user content and misconduct under state and federal law
- Understanding the laws governing SEO and SEM and their impact on e-commerce vendors, including major developments involving internet advertising and embedded and sponsored links
- AI, screen scraping and database protection
- Strategies for defending cybersecurity breach and data privacy class action suits
- Copyright and Lanham Act fair use, patentable subject matter, combating genericide, right of publicity laws governing the use of a person's images and attributes, initial interest confusion, software copyrightability, damages in internet and mobile cases, the use of icons in mobile marketing, new rules governing fee awards, and the applicability and scope of federal and state safe harbors and exemptions
- How to enforce judgments against foreign domain name registrants
- Valuing domain name registrations from sales data
- Compelling the disclosure of the identity of anonymous and pseudonymous tortfeasors and infringers
- Exhaustive statutory and case law analysis of the Digital Millennium Copyright Act, the Communications Decency Act (including exclusions created by FOSTA-SESTA), the Video Privacy Protection Act, and Illinois Biometric Privacy Act
- Analysis of the CLOUD Act, BOTS Act, SPEECH Act, Consumer Review Fairness Act, N.J. Truth-in-Consumer Contract, Warranty and Notice Act, Family Movie Act and more
- Practical tips, checklists and forms that go beyond the typical legal treatise
- Clear, concise, and practical analysis

AN ESSENTIAL RESOURCE FOR ANY INTERNET AND MOBILE, INTELLECTUAL PROPERTY OR DATA PRIVACY/ CYBERSECURITY PRACTICE

E-Commerce & Internet Law is a comprehensive, authoritative work covering law, legal analysis, regulatory issues, emerging trends, and practical strategies. It includes practice tips and forms, nearly 10,000 detailed footnotes, and references to hundreds of unpublished court decisions, many of which are not available elsewhere. Its unique organization facilitates finding quick answers to your questions.

The updated new edition offers an unparalleled reference and practical resource. Organized into five sectioned volumes, the 59 chapters cover:

- Sources of Internet Law and Practice
- Intellectual Property
- Licenses and Contracts
- Data Privacy, Cybersecurity and Advertising
- The Conduct and Regulation of E-Commerce
- Internet Speech, Defamation, Online Torts and the Good Samaritan Exemption
- Obscenity, Pornography, Adult Entertainment and the Protection of Children
- Theft of Digital Information and Related Internet Crimes
- Platform liability for Internet Sites and Services (Including Social Networks, Blogs and Cloud services)
- Civil Jurisdiction and Litigation

Distinguishing Features

- Clear, well written and with a practical perspective based on how issues actually play out in court (not available anywhere else)
- Exhaustive analysis of circuit splits and changes in the law combined with a common sense, practical approach for resolving legal issues, doing deals, documenting transactions and litigating and winning disputes
- Covers laws specific to the Internet and explains how the laws of the physical world apply to internet and mobile transactions and liability risks
- Addresses both law and best practices
- Comprehensive treatment of intellectual property, data privacy and mobile and Internet security breach law

SUMMARY OF CONTENTS

"Should be on the desk of every lawyer who deals with cutting edge legal issues involving computers or the Internet."
Jay Monahan
General Counsel, ResearchGate

****
ABOUT THE AUTHOR
****

IAN C. BALLON

Ian Ballon is Co-Chair of Greenberg Traurig LLP's Global Intellectual Property and Technology Practice Group and is a litigator based in the firm's Silicon Valley and Los Angeles offices. He defends data privacy, cybersecurity breach, TCPA, and other Internet and mobile class action suits and litigates copyright, trademark, patent, trade secret, right of publicity, database and other intellectual property matters, including disputes involving Internet-related safe harbors and exemptions and platform liability.

Mr. Ballon was the recipient of the 2010 Vanguard Award from the State Bar of California's Intellectual Property Law Section. He also has been recognized by *The Los Angeles and San Francisco Daily Journal* as one of the Top 75 Intellectual Property litigators, Top Cybersecurity and Artificial Intelligence (AI) lawyers, and Top 100 lawyers in California.

In 2017 Mr. Ballon was named a "Groundbreaker" by *The Recorder* at its 2017 Bay Area Litigation Departments of the Year awards ceremony and was selected as an "Intellectual Property Trailblazer" by the *National Law Journal*.

Mr. Ballon was named as the Lawyer of the Year for information technology law in the 2019, 2018, 2016 and 2013 editions of *The Best Lawyers in America* and is listed in Legal 500 U.S., The Best Lawyers in America (in the areas of information technology and intellectual property) and Chambers and Partners USA Guide in the areas of privacy and data security and information technology. He also serves as Executive Director of Stanford University Law School's Center for E-Commerce in Palo Alto.

Mr. Ballon received his B.A. *magna cum laude* from Tufts University, his J.D. *with honors* from George Washington University Law School and an LLM in international and comparative law from Georgetown University Law Center. He also holds the C.I.P.P./U.S. certification from the International Association of Privacy Professionals (IAPP).

In addition to *E-Commerce and Internet Law: Treatise with Forms 2d edition*, Mr. Ballon is the author of *The Complete CAN-SPAM Act Handbook* (West 2008) and *The Complete State Security Breach Notification Compliance Handbook* (West 2009), published by Thomson West (www.IanBallon.net).

He may be contacted at BALLON@GTLAW.COM and followed on Twitter and LinkedIn (@IanBallon).

Contributing authors: Parry Aftab, Ed Chansky, Francoise Gilbert, Tucker McCrady, Josh Raskin, Tom Smedinghoff and Emilio Varanini.

NEW AND IMPORTANT FEATURES FOR 2019

- A comprehensive analysis of the **California Consumer Information Privacy Act**, **California's Internet of Things (IoT) security statute**, **Vermont's data broker registration law**, **Ohio's safe harbor** for companies with written information security programs, and other new state laws governing cybersecurity (chapter 27) and data privacy (chapter 26)
- An exhaustive analysis of **FOSTA-SESTA** and what companies should do to maximize CDA protection in light of these new laws (chapter 37)
- The **CLOUD Act** (chapter 50)
- Understanding **the TCPA after *ACA Int'l*** and significant new cases & circuit splits (chapter 29)
- Fully updated **50-state compendium** of security breach notification laws, with a **strategic approach** to handling notice to consumers and state agencies (chapter 27)
- **Platform liability and statutory exemptions and immunities** (including a comparison of "but for" liability under the CDA and DMCA, and the latest law on secondary trademark and patent liability) (chapter 49)
- Applying **the single publication rule** to websites, links and uses on social media (chapter 37)
- The complex array of potential liability risks from, and remedies for, **screen scraping, database protection and use of AI to gather data and information online** (chapter 5)
- State online dating and revenge porn laws (chapter 51)
- **Circuit splits on Article III standing in cybersecurity litigation** (chapter 27)
- Revisiting **sponsored link, SEO and SEM practices and liability** (chapter 9)
- **Website and mobile accessibility** (chapter 48)
- **The Music Modernization Act's Impact on copyright preemption and DMCA protection for pre-1972 musical works** (chapter 4)
- **Compelling the disclosure of passwords and biometric information to unlock a mobile phone, tablet or storage device** (chapter 50)
- Cutting through the jargon to make sense of ***clickwrap*, *browsewrap*, *scrollwrap* and *sign-in wrap* agreements (and what many courts and lawyers get wrong about online contract formation)** (chapter 21)
- The latest case law, trends and strategy for **defending cybersecurity and data privacy class action suits** (chapters 25, 26, 27)
- **Click fraud** (chapter 28)
- Updated **Defend Trade Secrets Act** and UTSA case law (chapter 10)
- **Drafting enforceable arbitration clauses and class action waivers** (with new sample provisions) (chapter 22)
- **Applying the First Sale Doctrine to the sale of digital goods and information** (chapter 16)
- **The GDPR, ePrivacy Directive and transferring data from the EU/EEA** (by Francoise Gilbert) (chapter 26)
- **Patent law** (updated by Josh Raskin) (chapter 8)
- **Music licensing** (updated by Tucker McCrady) (chapter 17)
- **Mobile, Internet and Social Media contests & promotions** (updated by Ed Chansky) (chapter 28)
- **Conducting a risk assessment and creating a Written Information Security Assessment Plan (WISP)** (by Thomas J. Smedinghoff) (chapter 27)