CORPORATE LAW AND PRACTICE
Course Handbook Series
Number B-2308

Ethics in Social Media 2017

Chair
Richard Raysman

To order this book, call (800) 260-4PLI or fax us at (800) 321-0093. Ask our Customer Service Department for PLI Order Number 186237, Dept. BAV5.

Practising Law Institute
1177 Avenue of the Americas
New York, New York 10036

1

Technology Law in the Digital Age: A Regularly-Updated Digest of Notable Developments (April 2016)

Submitted by:
Richard Raysman
Holland & Knight LLP

Table of Contents

The secure establishment, in business and personal use, of the Internet and other modes of accessing information in digital form has raised novel and complex legal issues for today's technology and intellectual property lawyers. The fast pace of this "information highway" stands in stark contrast to the traditional landscape of commercial transactional and intellectual property law. Many existing laws were not designed to deal with a technology that disseminates information at the speed, with the convenience, and to the mass audience now possible in the modern information age. Just as the number of Internet and wireless device users continues to multiply, the number of legal issues of first impression continues to make technology law an exciting and engaging area of practice.

The information technology industry is constantly changing, and its evolution continues apace. New data and media formats, new applications and services, and new methods to access and store data are constantly introduced into the business and consumer markets. It is not only important for the technology law attorney to keep abreast of these changes, but also to the changes in the law. As such, this white paper provides a concise resource of some of the latest legal developments in technology law, data security and privacy, and e-commerce and licensing. For a more thorough discussion and consideration of these issues, please refer to *Computer Law: Drafting and Negotiating Forms and Agreements*, co-authored by Richard Raysman and Peter Brown (Law Journal Press 1984-2014), *Intellectual Property Licensing: Forms and Analysis* (Law Journal Press 1999-2014), co-authored by Richard Raysman, Edward A. Pisacreta, Kenneth A. Adler and Seth H. Ostrow, and *Emerging Technologies and the Law: Forms & Analysis* (Law Journal Press 1994-2014), co-authored by Richard Raysman, Peter Brown, Jeffrey D. Neuburger and William E. Bandon, III.

For a compendium of recent articles and alerts that discuss technology law issues in greater depth, please visit the firm's website at www.hklaw.com and the Digital Technology & E-Commerce Blog.

COPYRIGHT AND DIGITAL CONTENT

Information technology has revolutionized the methods for creating, reproducing, and disseminating copyrighted works and has consequently opened the door to instances of wide-scale copyright infringement. Combined with powerful software applications, the Internet is an ideal medium, in terms of its ease of use and wide audience, for replicating copyrighted works. With the simple push of a button or a click of a mouse, a user can upload information, making it available to a worldwide audience, or extract and download information posted on the Web. Services or products that facilitate access to websites throughout the world can significantly magnify the effects of otherwise immaterial infringing activities.

When copyrighted information is made available online without the permission of the copyright holder, two questions may arise: Who is liable? Under what legal theory (e.g., copyright infringement, DMCA violation, etc.)? A party who makes or distributes unauthorized copies of copyrighted works may be a direct infringer, but other participants, such as electronic bulletin board operators, website operators, bloggers, social network sites, peer-to-peer networks, video sharing sites, and ISPs, can potentially be liable as contributory or vicarious infringers.

Modern Distribution of Digital Content

- **American Broadcasting Companies, Inc. v. Aereo, Inc.** – Aereo, Inc. sold a service that allowed its subscribers to watch television programs over the Internet at about the same time as the programs are broadcast over the air. When a subscriber wants to watch a show that is currently airing, he selects the show from a menu on Aereo's website. Aereo's system, which consists of thousands of small antennas and other equipment housed in a centralized warehouse, responds roughly as follows: A server tunes an antenna, which is dedicated to the use of one subscriber alone, to the broadcast carrying the selected show. A transcoder translates the signals received by the antenna into data that can be transmitted over the Internet. A server saves the data in a subscriber-specific folder on Aereo's hard drive and begins streaming the show to the subscriber's screen once several seconds of programming have been saved. The streaming continues, a few seconds behind the over-the-air broadcast, until the subscriber has received the entire show. In the 2014 term, the Supreme Court held that Aereo's service both (a) "performed" the copyrighted works within the meaning of the Copyright Act, and (b) "performed" the works "publicly"

within the meaning of the Transmit Clause of the Act.[1] Accordingly, Aereo was committing copyright infringement by retransmitting the signals of the broadcaster's without consent. After two Supreme Court cases holding that the rechanneling of broadcaster signals rendered the entities doing the rechanneling as "viewers" and not "performers" the Act was amended to "completely overturn[]" the "narrow construction" employed in those cases.[2] In relevant part, the Act was amended so that *both* the broadcaster and the viewer "perform" the work because they both show the program's images and make audible the program's sounds. The court likewise held that Aereo performed the works publicly under the meaning of the Transmit Clause. Among other reasons for holding that Aereo performed the copyrighted works publicly, the court held that: (1) the stated objectives of the Act amendments should not yield to the unique nature of the Aereo transmission system given that Aereo has a commercial objective and its service does not deliver programming to its viewers in any way so as to alter the viewing experience (2) the statutory language of the Act indicates that the Transmit Clause refers to multiple, discrete transmissions (as Aereo would do any time any 2 or more of its subscribers were watching the same program) and not a single transmission; (3) and that Aereo facilitates the performance of the works publicly because its subscribers may receive the same programs at different times and locations, and under the Transmit Clause "the public" need not to be situated together, spatially or temporally. Rather, a work is transmitted publicly under this clause "whether the members capable of receiving the performance … receive it in the same place or in separate places and at the same

1. American Broadcasting Companies, Inc. v. Aereo, Inc., 134 S. Ct. 2498 (2014); see 17 U.S.C. § 106(4) ("[T]he owner of [a] a copyright … has the exclusive right to … perform the copyrighted work publicly.").
2. See, e.g., Teleprompter Corp. v. Columbia Broadcasting System, Inc., 415 U.S. 394 (1974) (provider that carried broadcast signals into subscribers' homes from hundreds of miles away considered a "viewer" and not a "performer" of the signals because the reception and rechanneling is, 408-09 "essentially a viewer function, irrespective of the distance between the broadcasting station and the ultimate viewer"); Fornightly Corp. v. United Artists Television, Inc., 392 U.S. 390, 398-400 (1968) (system that carried copyrighted local TV signals into subscribers' homes via antennas on hills above those cities does not "perform" the signals because they do not edit the programs, nor procure the programs to thereafter propagate them to the public; rather, the system falls "on the viewer's side of the line" by using "amplifying equipment" similar to how a viewer provides the same equipment").

time or at different times." The Supreme Court decision arose after a series of decisions at the federal appellate level that conflicted on whether Aereo's service violated the Act.[3]

---

3. See WNET, Thirteen v. Aereo, Inc., 712 F.3d 676 (2d Cir. 2013), *reh'g en banc denied*, 722 F.3d 500 (2d Cir. 2013). In *WNET, Thirteen*, The court found that the defendant's system, like the RS-DVR system in the controlling precedent, Cartoon Network LP, LLLP v. CSC Holdings, Inc., 536 F.3d 121 (2d Cir. 2008) ("*Cablevision*") created unique, user-requested copies that were generated by their own individually rented antenna and transmitted only to the particular user that created them and, therefore, its performances were nonpublic. The court stated that *Cablevision* expressly rejected the argument, advanced again in this case, that the mere fact that a content provider is making a given work available to all of its subscribers results in a public performance. The appeals court reiterated that, looking at the "Transmit Clause" of the Copyright Act, if a transmission is "capable of being received by the public" the transmission is a public performance; if the potential audience of the transmission is only one subscriber, the transmission is not a public performance, and private transmissions to multiple parties should not be aggregated, except when private transmissions are generated from the same copy of the work. In *Cablevision*, a cable TV company's remote storage digital video recorder (RS-DVR) system that would allow subscribers the option to record television programming on the company's own servers for subsequent personal viewing does not amount to direct copyright infringement. The court ultimately granted summary judgment in favor of the defendant-cable company because the proposed RS-DVR did not directly infringe the plaintiff's exclusive rights to reproduce and publicly perform their copyrighted works. As to claims of infringement of the exclusive right of public performance, the court concluded that the RS-DVR playback involved a nonpublic performance because the system would only make playback transmissions to one subscriber using a unique copy produced by that subscriber and, as such, the universe of people capable of receiving transmissions of a program was the single subscriber and could not be considered performances "to the public." *Compare* WNET, Thirteen, 712 F.3d at 677; Hearst Stations Inc v. Aereo, Inc., 977 F. Supp. 2d 32 (D. Mass. 2013) (transmitting a performance to a single user via a single antenna is a private performance under the Copyright Act) *with* Fox Television Stations, Inc. v. Film On X LLC, 956 F. Supp. 2d 30 (D.D.C. 2013) (internet transmission TV service with technology materially identical to Aereo did infringe the public performance rights under the "Transmit Clause" because in making its technology to available to any member of the public, it performs it publicly under the Act, a right which is afforded to the copyright owner); Fox Television Stations Inc. v. BarryDriller Content Systems PLC, 915 F. Supp. 2d 1138 (C.D. Cal. 2012) (internet retransmission TV service, akin to Aereo, likely infringes broadcaster's exclusive right to make public transmissions of their copyrighted works; court issues preliminary injunction halting the service within the boundaries of the Ninth Circuit); see also Fox Broadcasting Co., Inc. v. Dish Network, LLC, 723 F.3d 1067 (9th Cir. 2013) (satellite television distributor using a DVR that allowed users to skip commercials aired during broadcast networks programming did not constitute direct or secondary copyright infringement). WPIX, Inc. v. ivi, Inc., 691 F.3d 275 (2d Cir. 2012) (affirming preliminary injunction and holding that online live TV streaming service is not a "cable

- **Garcia v. Google, Inc.** – The Ninth Circuit has recently held that even just the physical portion of a performance in a motion picture can be copyrightable by the actor whom gives the performance, irrespective of whether the physical portion of a performance can be considered "original."[4] The case dealt with an actress whose lines were overdubbed in a film different from the one she thought she was performing. It held that the actress was entitled entitled to injunction under DMCA because the film was explosive "Innocence of Muslims" which enraged Muslim world and led to death threats against the actress. The actress received the injunction after Google refused to take down the video from YouTube because her performance, despite including overdubbed lines, evinced a copyrightable interest because she nonetheless contributed a minimal degree of creativity to the film through body language, facial expression and other reactions.

  A subsequent decision of the Ninth Circuit agreed that Garcia possessed a likelihood of success on the merits of her claim to a copyrightable interest in her performance in the "Innocence of Muslims."[5] The Garcia II court also discussed the intersection between the performer's assertion of a copyrightable interest in her performance and the often competing doctrines of work for hire and implied license. As noted in the opinion, Garcia's performance would vest in the director of "Innocence of Muslims" if she was his employee and acted in her employment capacity or was an independent contractor who transferred her interest in writing.[6] In Garcia II, the court held that Garcia was hired for a specific task, worked only three days, received no other health or traditional employment benefits, and did not sign a written agreement transferring the copyright to the director. Therefore, she could not qualify as a traditional employee under the work for hire doctrine.

  As for the argument that Garcia conveyed a nonexclusive license to the director, the court agreed that such a license exists and can be implied from conduct when a plaintiff creates a work at defendant's request and hands it over, intending that the defendant copy and distribute it. The court agreed that Garcia had granted an

---

system" entitled to a compulsory license under § 111 of the Copyright Act because they provide nationwide—and arguably global —services).

4. 743 F.3d 1258 (9th Cir. 2014).
5. 766 F.3d 929 (9th Cir. 2014).
6. See also Cmty. for Creative Non-Violence v. Reid, 490 U.S. 730 (1989).

implied license since her performance would be otherwise unusable to the director.[7] *However*, the Garcia II court noted that a broad implied license "isn't unlimited," because Garcia's performance ended up in a "film" that differed radically from what Garcia could have imagined, the performance could not have been authorized by an implied license. The case will be reheard before an en banc panel of the same court in 2015.[8]

- **United States v. Anderson** – Defendant Roosevelt Anderson Jr. was convicted of criminal copyright infringement under 17 U.S.C. § 506(a)(1)(A) and 18 U.S.C. § 2319(b)(1) after he sold stolen Adobe software by managing to circumvent the product key requirements designed to authenticate the software.[9] He was sentenced to two years in prison and was ordered to pay nearly $250,000 in restitution to Adobe. Anderson appealed in part on the grounds that the jury instruction on the criminal copyright willfulness standard improperly suggested that the jury could convict him without specific intent to violate the law.[10] His appeal was denied, as the Ninth Circuit agreed with the trial court that the defendant's proposed willfulness instruction added additional elements and had the potential create confusion. Although the use of the qualifier "may" in the first sentence of the instruction was "vague" and a mischaracterization of the requisite *mens rea* to convict, "when viewed in its entirety," the instruction was not misleading or inadequate insofar as it required the defendant to know that his actions constituted *copyright infringement, and not merely a violation of a legal duty*.[11]

---

7. See also 17 U.S.C. § 106(4) (but for the existence of a robust license, the performer could prevent the author from exercising his exclusive right to show the work to the public).
8. Garcia v. Google, Inc., 771 F.3d 647 (9th Cir. 2014) (granting rehearing).
9. 741 F.3d 938 (9th Cir. 2013).
10. A variety of courts have weighed in on the requisite *mens rea* in the context of criminal copyright infringement. See, e.g., Cheek v. United States, 498 U.S. 192 (1991) (a copyright is infringed willfully when the defendant intentionally violated a known legal duty); Screws v. United States, 325 U.S. 91 (1945) (a defendant can only be found guilty if he evinces a motive to violate that which the statute protects; something more is required than doing the act proscribed by the statute); United States v. Heilman, 614 F.2d 1133 (7th Cir. 1980) (infringement of the copyright in the context of willfulness requires acts taken with a purpose to deprive the copyright holder of the interests protected by its copyright).
11. See U.S. v. Anderson, 741 F.3d 938; but see United States v. Liu, 731 F.3d 982 (9th Cir. 2013) (jury instruction hinting that a jury could convict a defendant of

- **Capitol Records, LLC v. ReDigi Inc.** – Digital music files, lawfully made and purchased, may not be resold by users through an online used digital music marketplace under the first sale doctrine.[12] The court granted the plaintiff's motion for summary judgment, ruling that defendant, the operator of an online digital music marketplace, was liable for the direct and secondary infringement of the plaintiff's reproduction and distribution rights. The court found that the reproduction right was necessarily implicated when a digital music file was embodied in a new material object following its transfer over the internet onto a new hard drive. The court rejected the defendant's argument that its service "migrates" a file from a user's computer to its Cloud Locker, so that the same file is transferred to its server and no copying occurs. Rather, the court ruled that even accepting defendant's description of the process, "the fact that a file has moved from one material object – the user's computer – to another – the ReDigi server – means that a reproduction has occurred. Similarly, when a ReDigi user downloads a new purchase from the ReDigi website to her computer, yet another reproduction is created. It is beside the point that the original phonorecord no longer exists. It matters only that a new phonorecord has been created." The court also held that the sale of "used" digital music files on the defendant's site violated the copyright owners' distribution right. The court rejected the defendant's affirmative defenses, concluding that ReDigi's reproduction and distribution of the plaintiff's copyrighted works fell "well outside" the fair use defense. While the record company notably admitted that uploading to and downloading from a cloud-based cyberlocker for storage and personal use was a protected fair use, the court agreed with the plaintiff that the uploading to and downloading from the cloud locker incident to sale was not "transformative" and fell outside the ambit of fair use. Regarding the first sale defense (applicable to the right of distribution, not reproduction), the court

---

criminal copyright infringement without a finding that he knew his actions were unlawful was not harmless error; conviction was vacated and the case remanded). The *Anderson* court also noted that there was "overwhelming evidence that Anderson acted with the requisite knowledge that his actions were unlawful, including his admissions that he: (a) resorted to selling unauthorized software after realizing that he did not have sufficient resources to pursue a legitimate deal with Adobe; (b) had been informed by his customers that was he was doing was illegal, though this did not deter him, and (c) knew that his customers were not using the discs for backup purpose. Anderson, 741 F.3d at 948-49.

12. Capitol Records, LLC v. ReDigi Inc., 934 F. Supp. 2d 640 (S.D.N.Y. 2013).

found that the defendant's service did not qualify because ReDigi users were not reselling the same music file that was originally created when users downloaded a song from iTunes: "[R]ather, it is distributing reproductions of the copyrighted code embedded in new material objects, namely, the ReDigi server in Arizona and its users' hard drives. The first sale defense does not cover this any more than it covered the sale of cassette recordings of vinyl records in a bygone era."

- **Agence France Press v. Morel** – Twitter's terms of use, which grant ownership of content to the user and license to Twitter some limited usage rights, do not grant a license to third party news organizations to remove photographic content from Twitter and license it to other news outlets and photo services without the consent of the copyright holder.[13] The court initially granted the plaintiff's motion for summary judgment that the defendant AFP and the Washington Post were liable for direct copyright infringement of the subject photographs, but found material issues of fact with respect to secondary liability claims and DMCA safe harbor defenses alleged by another defendant-photo service. The court rejected AFP's argument that it was a third-party beneficiary to the limited license grant to Twitter, concluding that the Twitter terms were not intended to confer a benefit on the world-at-large to remove content from Twitter and commercially distribute it. The court also ruled that the statement within Twitter's terms such as "what's yours is yours – you own your content" would be meaningless if the terms allowed unrestricted licensing to third parties, and that it was immaterial that Twitter encourages and permits broad re-use (i.e., retweets) of content, since such actions do not "necessarily require that AFP was granted an unrestricted license to remove the Photos-at-Issue from Twitter and license them to others." Regarding statutory damages under the Copyright Act, the court rejected the plaintiff's expansive view of the 17 U.S.C. § 504, and held that it was Congress's intent to restrict statutory damages to a single award per work, per infringer;[14] similarly, under the

13. Agence France Press v. Morel, 934 F. Supp. 2d 547 (S.D.N.Y. 2013).
14. In further proceedings, the court clarified its holding regarding statutory damages and ruled that the plaintiff was, at most, entitled to receive one award of statutory damages per work infringed in this action. The court held that the liability of an individual or group of individuals for the infringement of any single work could not be multiplied by the number of separate end-point infringers with whom that individual or group was jointly liable, and that a plaintiff seeking statutory damages for

DMCA's provisions for removal of copyright management information, the court concluded that damages should be assessed per violation (i.e., based on AFP and other defendants' actions in uploading or distributing the photos-at-issue, regardless of the number of recipients of these images).

- **UMG Recordings, Inc. v. Augusto** – The Copyright Act's first sale doctrine allows an individual to resell promotional music CDs previously sent to industry insiders, despite the fact that the CDs bore labels with language that purportedly "licensed" use of the CD by the recipient.[15] The appeals court affirmed the defendant-online reseller's motion for summary judgment on the plaintiff-record company's copyright infringement claim. The court concluded that, under all the circumstances of the CDs' distribution, the recipients were entitled to use or dispose of them in any manner they saw fit, and UMG did not enter a license agreement for the CDs with the recipients. The court noted that the promotional CD were mailed without any prior arrangements, were not numbered and no attempt was made to track their usage, and as such, the record company's transfer of unlimited possession under these circumstances effected a gift or a sale within the meaning of the first sale doctrine. Interestingly, in dicta, the court commented on basic contract law concerning an offeree's silence equaling acceptance of an offer: "It is one thing to say, as the [CD label] does, that 'acceptance' of the CD constitutes an agreement to a license and its restrictions, but it is quite another to maintain that 'acceptance' may be assumed when the recipient makes no response at all."
- **Luvdarts LLC v. AT&T Mobility LLC** – Wireless carriers that deploy technology that allows for the free transfer of MMS content between users and do not block or filter allegedly infringing transfers are not liable for secondary copyright infringement.[16] The appeals court affirmed the lower court's dismissal of the plaintiff's claims. The court stated that the plaintiffs failed to allege that the carriers had the necessary specific knowledge of ongoing infringement to sustain a contributory infringement claim. The court also

---

copyright infringement may not multiply the number of per-work awards available in an action by pursuing separate theories of individual liability against otherwise jointly liable defendants. See Agence France Press v. Morel, 934 F. Supp. 2d 584 (S.D.N.Y. 2013).

15. UMG Recordings, Inc. v. Augusto, 628 F.3d 1175 (9th Cir. 2011).
16. Luvdarts LLC v. AT&T Mobility LLC, 2013 710 F.3d 1068 (9th Cir. 2013).

dismissed the plaintiff's vicarious infringement claims, finding that the defendants had no ability to control or supervise MMS transmissions and the plaintiff failed to allege facts that plausibly showed how the defendants could implement an effective system of supervision.

- **In re Application of Cellco Partnership d/b/a Verizon Wireless** – A cellular telephone provider is not required to pay ASCAP a public performance license fee for ringtones downloaded and used by its customers.[17] The court granted summary judgment to the provider and found that while it is undisputed that the act of reproducing and distributing a ringtone implicates other reproduction and distribution rights created by the Copyright Act, the transmission of a ringtone to a customer's cellular telephone is not a "public performance" of a musical work as defined by the Copyright Act. As to the provider's contributory liability, the court stated that when a ringtone plays on a cellular telephone, even in public, the user is exempt from copyright liability (and thus, the provider is not liable secondarily), because a ringtone plays only in the presence of the "normal circle of a family and its social acquaintances" and not for a "commercial advantage." As for the direct liability claims, the court concluded that the provider's only role in the playing of a ringtone was the sending of a signal to

17. In re Application of Cellco Partnership d/b/a Verizon Wireless, 663 F. Supp. 2d 363 (S.D.N.Y. 2009). See also United States v. American Society of Composers, Authors & Publishers, 599 F. Supp. 2d 415 (S.D.N.Y. 2009) (telecom company argued that its use of ASCAP music in previews to allow users to hear snippets before downloading ringtones was fair use and therefore, it does not owe ASCAP royalty payments for the previews; court found that the applicant's use of previews was not transformative because, among other reasons, the music segments used in applicant's previews were exact copies of ASCAP music and the previews, for the purpose of allowing its customers to sample a ringtone before purchasing it, could not fairly be described as "criticism, comment, news reporting, teaching . . . scholarship, or research"); United States v. ASCAP, 627 F.3d 64 (2d Cir. 2010) (appeals court affirmed lower court ruling that a download of a musical work does not constitute a public performance of that work, but vacated the district court's assessment of fees for the blanket ASCAP licenses sought by the two Internet companies and remanded for further proceedings that would yield a royalty rate that reflects the varying nature of the companies' music use); Kernal Records Oy v. Mosley, 794 F. Supp. 2d 1355 (S.D. Fla. 2011) (publishing a musical work on a website without restrictions in Australia was an act tantamount to global and simultaneous publication of the work, bringing the work within the definition of a "United States work" under § 101(1)(C) and subject to § 411(a)'s registration requirement).

alert a customer's telephone to an incoming call, with the signal being the same whether the customer has downloaded a ringtone or not, an activity that was not sufficiently connected to the alleged public performance of the ringtone to implicate any copyright liability.

- **A.V. v. iParadigms, LLC –** An online anti-plagiarism service used by educational institutions that compares student papers to content available on the Internet and archives student submissions for future comparisons is protected from copyright infringement claims by the fair use defense.[18] The appeals court affirmed the lower court's grant of summary judgment to the defendant on the plaintiffs-student authors' copyright claims stemming from the copying and allegedly unauthorized archiving of their papers into the defendant's plagiarism database. In conducting a fair use analysis, the court found the defendant's use to be transformative, making only limited use of the student works' expressive or creative content when it compared the works to existing electronic sources. The court also found that the defendant's use caused no harm to the market value of the students' works because the site's comparison analysis did not amount to a market substitute for the students' papers.

  This is a notable digital fair use decision since the court confirmed and sharpened several aspects of the defense. The court made clear that the disputed use of copyrighted material should be weighed alongside the transformative nature of the new work and that

18. A.V. v. iParadigms, LLC, 562 F.3d 630 (4th Cir. 2009). See also Christen v. iParadigms LLC, 2010 WL 3063137 (E.D. Va. Aug. 4, 2010) (conversion claims based upon uploading of students' papers to plagiarism service preempted by Copyright Act); Hollander v. Steinberg, 419 Fed. Appx. 44 (2d Cir. 2011) (summary order) (attorneys who attached copies of the plaintiff's online essays in support of legal papers filed in two separate judicial proceedings were protected from copyright infringement by the fair use defense because the essays were submitted to evince the workings of the plaintiff's state of mind and such non-commercial use could not realistically be viewed as negatively impacting the market for the essays) Northland Family Planning Clinic Inc. v. Center for Bio-Ethical Reform, 868 F. Supp. 2d 962 (C.D. Cal. 2012) (parody video that copied large portions of original material was deemed fair use); SOFA Entertainment, Inc. v. Dodger Productions, Inc., 709 F.3d 1273 (9th Cir. 2013) (use of 7-second clip of the Ed Sullivan Show in a musical about the Four Seasons to mark a historical point in the band's career was fair use); but see Balsley v. LFP Inc., 691 F.3d 747 (6th Cir. 2012) (publication of old, racy images of local reporter without authorization for inclusion in an adult magazine is not fair use).

unduly emphasizing the commercial motivation of the copier can lead to an overly restrictive view of fair use. Also, the court recognized that, like Google's image search function, which uses thumbnails of copyrighted images, a new use that does not add anything to the copyrighted work can still be transformative in function or purpose.[19]

- **Meshwerks, Inc. v. Toyota Motor Sales U.S.A., Inc. –** Unadorned digital models of cars that depict the three-dimension object in a two-dimensional digital medium for the purpose of Web-based advertisements were merely replicated images and not sufficiently original to warrant copyright protection.[20] The appeals court affirmed the lower court's finding of summary judgment in favor of the defendant, finding that the plaintiff's digital modeling images were "not so much independent creations as (very good) copies of [the] vehicles" and thus were not original, copyrightable matter. In discussing originality, the court found that the models depicted nothing more than unadorned vehicles and the plaintiff made no decisions regarding lighting, shading, background, or any new expressions subject to copyright protection. The court commented that effort alone was not enough to make the resultant digital model "original" and therefore copyrightable and the fact that a work in one medium has been copied from a work in another medium "does not render it any less a 'copy'."

Contributory and Vicarious Copyright Infringement

When a widely-shared service or application is used to commit infringement, it may be impossible to enforce rights in the protected work effectively against all direct infringers. Often, the only practical alternative is to seek legal remedies against the creator or distributor of the infringing device for secondary liability on a theory of contributory or vicarious infringement. Contributory and vicarious infringement are predicated on a direct infringement. Generally speaking, "[o]ne infringes contributorily by intentionally inducing or encouraging direct infringement, and infringes vicariously by profiting from

19. See also Scholz Design, Inc. v. Sard Custom Homes, LLC, 691 F.3d 182 (2d Cir. 2012) (architectural drawings are not required to contain sufficient detail to allow for construction in order to receive Copyright Act protection as a pictorial work; plaintiff's claims derive from the general copyright law and not from the AWCPA, which has no relevance to the suit).
20. Meshwerks, Inc. v. Toyota Motor Sales U.S.A., Inc., 528 F.3d 1258 (10th Cir. 2008).

direct infringement while declining to exercise a right to stop or limit it."[21] Put another way, a contributory infringer is a party who, with knowledge of the direct infringement, induces, causes or materially contributes to the activity of the direct infringer.

However, certain legal doctrines, such as the fair use defense, permit the use of copyrighted works without the copyright owner's consent under certain situations. As detailed below, a number of decisions have been issued recently that deal with a fair use defense raised in the context of digitizing books and permitting users to then search the books via databases.

- **Authors Guild, Inc. v. Hathi Trust** – the Second Circuit ruled in *Authors Guild, Inc v. Hathi Trust* that digitization of copyrighted works by a collection of universities to permit full-text searching and to provide print-disabled patrons with versions of all works contained in the digital archive in forms accessible to them each constituted fair use.[22] The full-text search function was found to be fair use because the full-text search did not substitute for the books being searched, as it did not permit access to the underlying text, and therefore the plaintiffs could not claim a cognizable economic harm under the Copyright Act since the search did not limit or impede the market for the work.[23] Moreover, the use of

21. Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 545 U.S. 913, 930 (2005); see UMG Recording, Inc. v. Escape Media Group, Inc. No. 11 Civ. 8407, 2014 WL 5089743 (S.D.N.Y. 2014) (employees of P2P network found liable for direct, vicarious and contributory infringement, as well as active inducement. because they had explicitly directed all of their employees to download the company's P2P software and then upload copyrighted music to it as a means of thereafter increasing scope and efficacy of the network to facilitate illegal downloads).
22. Authors Guild, Inc v. HathiTrust, 755 F.3d 87 (2d Cir. 2014). The HathiTrust digital library, unless the copyright holder permitted broader use, produced search results that show only the page numbers on which the search term is found, and the number of times the term appears on each page. Id. at 91. Moreover, the digital library does not display to the user any text of the copyrighted work, even in "snippet form." Id.
23. Id. at 99. This "economic harm" factor only applies when the use of the work is not transformative, as such a use is *per se* not a substitute for the original work. See, e.g., Campbell v. Acuff-Rose Music, Inc., 510 U.S. 569, 591 (1994) ("cognizable market harm" is limited to "market substitution"); NXIVM Corp. v. Ross Institute, 364 F.3d 471 (2d Cir. 2004) (stating that the relevant inquiry for purposes of economic harm is whether the secondary use "usurps the market of the original work"); see also White v. West Pub. Corp., — F. Supp. 2d —, 2014 WL 3057885 (S.D.N.Y. 2014) (legal publishers that placed searchable versions of an attorney's legal briefs did not infringe his copyrights because they made fair use of the works by transforming them into interactive legal research tools; Specifically, the publishers had reviewed, selected, converted, coded, linked and

the works by the universities was "transformative" under the Copyright Act because the result of a word search is "different in purpose, character, expression, meaning and message from the page (and the book) from which it is drawn. The decision of the universities to allow print-disabled persons to read the digitized works was likewise permitted under fair use. Although it was not considered transformative since its purpose (like the author's) was to find an audience to read the work, the Second Circuit nonetheless labeled it as fair use because (a) Congress had explicitly declared this purpose to exemplify fair use when drafting the relevant sections of the Copyright Act; and (b) permitting "print disabled" individuals to access the works would not hinder the market for the works.[24]

- **Elsevier Ltd. v. Chitika, Inc.** – An online advertising provider that was not familiar with the content of an allegedly infringing free download site and had not received any notice of infringing activity from the copyright holder was not liable for contributory copyright infringement.[25] The court granted the defendant's motion

---

identified the documents in a way that "add[] something new, with a further purpose or different character" than the original briefs); Case C-117/13, Technische Universität Darmstadt v. Eugen Ulmer K.G., ECLI:EU:C:2014:2196 (Sept. 11, 2014) (in a case involving a nearly identical fact pattern to *Hathi Trust*, the highest court of Europe, the European Court of Justice, held that libraries have the right to digitize books for use on reading terminals without the consent of copyright holders.

24. See, e.g., Sony Corp. of America v. Universal City Studios, Inc., 464 U.S. 417, 455, n.40 (1984) ("Making a copy of the copyrighted work for the convenience of a blind person is expressly identified by the House Committee report as an example of fair use[.]"; H.R. Rep. No. 94-1476, at 73 (1976), reprinted in 1976 U.S.C.C.A.N. 5659, 5686 (noting that making copies accessible for blind persons posed a "special instance illustrating the application of the fair use doctrine"). The court stated that "the present day market for books accessible to the handicapped is so insignificant that it is common practice in the publishing industry for authors to forgo royalties that are generated through the sale of books manufactured for the blind." Authors Guild, 755 F.3d at 103 (internal quotations omitted).
25. Elsevier Ltd. v. Chitika, Inc., 826 F. Supp. 2d 398 (D. Mass. 2011). See also Ark Promotions, Inc. v. Justin.tv, Inc, 904 F. Supp. 2d 541 (W.D.N.C. 2012) (plaintiff's one sentence allegation that defendant provides detailed instructions on its website directing users how to stream live video over the internet through its website does not adequately support a plausible claim that defendant is liable for inducement of copyright infringement); Liberty Media Holdings, LLC v. Tabora, No. 12-2234 (S.D.N.Y. July 9, 2012) (negligence claim against individual who allegedly permitted his roommate to engage in file sharing via a shared internet connection is preempted by the Copyright Act; the imposition of liability on one who knowingly contributes

to dismiss the contributory copyright infringement claim. The court also, in dicta, rejected the plaintiff's argument that the defendant "materially contributed to the infringement" merely because the shared advertising revenue made it easier for the website owner's infringement to be profitable.

- **Klein & Heuchan, Inc. v. CoStar Realty Information, Inc.** – An employer is neither contributorily or vicariously liable for copyright infringement due to the unauthorized use of a licensed database by one of its associates because the employer had no knowledge that its associate's use was unauthorized, did not materially contribute to the infringement and did not profit directly from its associate's use.[26] After a bench trial, the court found that the employer was entitled to a judgment of non-infringement. Regarding the vicarious liability claim, the court found that the avoidance of subscription fees may be sufficient to constitute "direct financial benefit," but that the associate did not share his access among other agents in the office and did not use the information in making any sales, such that the employer did not receive any direct financial benefit from the exploitation of the copyrighted material.
- **Arista Records LLC v. Usenet.com, Inc. –** A subscription-based global online bulletin board network that hosted downloadable text articles and unauthorized copies of music recordings was liable for copyright infringement, despite its claims that its service had substantial non-infringing uses.[27] The court granted

---

to a direct infringement by another is already protected under the doctrine of contributory infringement).

26. Klein & Heuchan, Inc. v. CoStar Realty Information, Inc., 707 F. Supp. 2d 1287 (M.D. Fla. 2010).
27. Arista Records LLC v. Usenet.com, Inc., 633 F. Supp. 2d 124 (S.D.N.Y. 2009). See also Arista Records LLC v. Lime Group, 784 F. Supp. 2d 398 (S.D.N.Y. 2011) (file-sharing service is liable for inducement of copyright infringement for intentionally encouraging and assisting rampant direct infringement by its users; massive scale of infringement committed by LimeWire users, and its knowledge of the infringement of its customers, supports a finding that LW intended to induce infringement; interestingly, the court denied the plaintiffs' motion for summary judgment on the contributory infringement claim stating that there existed a genuine issue of material fact as to whether LimeWire was "capable of substantial noninfringing uses" such that liability should not be imposed pursuant to the Sony-Betamax rule); Maverick Recording Co. v. Harper, 598 F.3d 193 (5th Cir. 2010) (17 U.S.C. §402(d) forecloses an innocent infringement defense for a music file-sharer liable for copyright infringement where copyright notices were placed

summary judgment to the music recording company plaintiffs against the defendant network. Comparing this case to the *Grokster* P2P litigation, the court found that the record was replete with instances of the defendant specifically engendering copyright infringement and targeting infringement-minded users to become subscribers of its service and that the "staggering scale of infringement" on the network made it more likely that the defendant condoned illegal use. The court found that the defendant liable for inducement of infringement by, among other things, openly and affirmatively seeking to attract former users of other notorious file-sharing services, explicitly acknowledging the availability of infringing uses through its service during customer interactions, and failing to use available tools to block access to limit copyright infringement on its servers. The court also found that the defendant was liable for direct, contributory and vicarious copyright infringement, rejecting the defendant's argument that it was merely a "passive conduit" that facilitated the exchange of content between users who uploaded infringing content and users who downloaded such content; rather, the court found that the defendant actively engaged in the process so as to satisfy the "volitional-conduct"

---

on CDs of the plaintiffs' works). But see David v. CBS Interactive Inc., No. 11-09437 (C.D. Cal. Feb. 19, 2013) (preliminary injunction against news and software download hub that published articles and videos about technological and legal issues surrounding file-sharing did not likely commit inducement of copyright infringement).

In certain cases, defendants have argued that a large award of statutory damages under the Copyright Act may be deemed to be punitive. In such cases, a court presumably has a duty to correct an unconstitutionally excessive verdict so that it conforms to the requirements of the due process clause, but in recent rulings, courts have declined to rule that large statutory damage awards under the Copyright Act was oppressive or unreasonable under Supreme Court precedent. See e.g., Capitol Records Inc. v. Thomas-Rasset, 692 F.3d 899 (8th Cir. 2012) (statutory damage award of $222,000 for willful infringement via music file sharing (i.e. $9,250 for each of the 24 works infringed) was not "so severe and oppressive as to be wholly disproportioned to the offense and obviously unreasonable,", the lower court erred in holding that the Due Process Clause allowed statutory damages of only $54,000; court rejected the application of the Supreme Court's punitive damages guideposts in the context of statutory damages awards); Sony BMG Music Entertainment, v. Tenenbaum, 660 F.3d 487 (1st Cir. 2011) (appeals court reversed the trial court's reduction on constitutional grounds of the original $22,500 per infringed song statutory damage award and reinstated the original $675,000 award, ruling that the lower court erred by unnecessarily reaching Tenenbaum's constitutional challenge to the award and bypassing the question of common law remittitur).

requirement for direct copyright infringement and the knowledge requirements inherent in contributory infringement.[28] Notably, the court also rejected the defendant's "Sony Betamax" defense, which purportedly provides immunity from contributory infringement if a service is capable of substantial non-infringing uses. In distinguishing the instant case from the Supreme Court's decision in *Sony Corp. of America v. Universal Studios, Inc.*,[29] the court noted that Sony's last meaningful contact with the product or the purchaser was at the point of purchase, after which it had no ongoing relationship with the product or its end-user, but that in this case, it was undisputed that the defendant maintained an ongoing relationship with their users.

- **Corbis Corporation v. Starr** – A company that was ultimately responsible for approving changes during the redesign of its website possessed the right and ability to limit the unauthorized usage of copyrighted photos and can be liable for vicarious copyright infringement.[30] The court granted summary judgment in favor of the copyright holder on its copyright claims. Despite the fact that the unauthorized images were supplied by the co-defendant Web designer, the court found that given the company's control over its website's content and its use of the images for marketing purposes (i.e., for its financial benefit), the company could be liable for vicarious infringement.

Copyright, Hot News, and News Aggregation

The online practices of certain blogs and news-oriented websites have been reexamined, particularly the practice of news aggregation,

---

28. But see Disney Enterprises, Inc. v. Hotfile Corp., 798 F. Supp. 2d 1303 (S.D. Fla. 2011) (remote storage website was not liable for direct copyright infringement simply because it gave users access to copyrighted material posted by others because it took no direct, volitional steps to upload copyrighted material or otherwise violate the plaintiff's rights; court refused to dismiss contributory claims based upon allegations that the website, through its business model, knowingly induced its users to infringe the plaintiffs' copyright).
29. 464 U.S. 417 (1984).
30. Corbis Corporation v. Starr, 2009 WL 2901308 (N.D. Ohio Sept. 2, 2009). See also Qassas v. Daylight Donut Flour Co., 2010 WL 2365472 (N.D. Okla. June 10, 2010) (website owner may be held liable for copyright infringement for copying a competitor's online content even though a third party developed the defendant's new website and the owner had no control over or decision-making authority concerning the content of the new website).

which is the presentation of the latest news headlines and story excerpts, along with a link to the originating site where the article first appeared. While some news aggregating sites copy a minimal amount of text and routinely display a prominent link to the original news source, other aggregators have purportedly engaged in certain acts of unlawful copying and misappropriation. The question arises whether a news organization has recourse, beyond federal copyright law, for misappropriation of its breaking news.

- **The Associated Press v. Meltwater U.S. Holdings, Inc.** – An online news aggregator and clipping service that scraped news articles and provided designated excerpts of those stories (including many AP stories), in reports sent to subscribers is not protected from copyright infringement claims by the fair use defense.[31] The court granted the AP summary judgment on its copyright claims based upon the defendant's partial copying of a number of its stories. The court found that the fair use factors weighed against the defendant because the defendant's copying of headlines and segments of AP stories (including the important story ledes) without adding any commentary in order to sell the content to subscribers was not transformative and did not justify allowing the defendant to "free ride on the costly news gathering and coverage work performed by other organizations" or avoiding paying licensing fees that give it "an unwarranted advantage over its competitors who do pay licensing fees." The court rejected the defendant's argument that its actions were akin to a search engine and should be protected by fair use, concluding rather that the defendant "is an expensive subscription service that markets itself as a news clipping service, not as a publicly available tool to improve access to content across the Internet." In short, the court found that the use of an algorithm to crawl and scrape content from the internet was "surely not enough to qualify as a search engine engaged in transformative work." Regarding the last fair use factor – the effect of the use on the potential

31. The Associated Press v. Meltwater U.S. Holdings, Inc., 931 F. Supp. 2d 537 (S.D.N.Y. 2013); see also Dow Jones & Co., Inc. v. Real-Time Analysis and News, Ltd., No. 14-CV-131 (JMF)(GWG), 2014 WL 5002092 (S.D.N.Y. Oct. 7, 2014) (in a question of fresh impression, district court holds that a "reasonable royalty," which in this instance refers to a fair licensing fee, and not the normal remedies such as lost profits or defendant's wrongful gain, as the latter in the context of misappropriation of trade secrets for the theft of "hot news," would be difficult to assess).

market – the court held that the defendant's business model relied on the systematic copying of protected expression and the sale of reports that competed directly with the copyright owner and its licensees and deprived that owner of a valid stream of licensing income. The court also rejected the defendant's implied license defense, concluding that the failure of AP's licensees to employ the robots.txt protocol to bar access by web crawlers did not give the defendant an implied license to copy and publish AP content: "what [the defendant] is suggesting would shift the burden to the copyright holder to prevent unauthorized use instead of placing the burden on the infringing party to show it had properly taken and used content."

- **Barclays Capital Inc. v. TheFlyOnTheWall.com –** A financial newsfeed website that posted, before the market opened, key information from proprietary, time-sensitive equity research reports distributed by several Wall Street investment firms to subscribing investors was liable for certain instances of copyright infringement but not hot news misappropriation.[32] The Second Circuit reversed the lower court and concluded that the plaintiffs' hot news claims were preempted by the Copyright Act because the defendant's acts at issue did not meet the exceptions for a "hot news" claim as recognized by *NBA v. Motorola, Inc.*, 105 F.3d 841 (2d Cir. 1997). Interestingly, the court commented that "unfairness alone is immaterial to a determination whether a cause of action for misappropriation has been preempted by the Copyright Act," and that "the adoption of new technology that injures or destroys present business models is commonplace." The court questioned the five-part

32. Barclays Capital Inc. v. TheFlyOnTheWall.com, 650 F.3d 876 (2d Cir. 2011). See also Agora Financial, LLC v. Samler, 725 F. Supp. 2d 291 (D. Md. 2010) (federal magistrate concludes "hot news" misappropriation claims are limited to claims in which the material at issue is factual information or material that is otherwise not protectable under the Copyright Act; while plaintiffs may be able to protect their "original" investment recommendations under federal copyright law, they cannot protect these recommendations under a "hot news" misappropriation theory). But see BanxCorp v. Costco Wholesale Corp., 723 F. Supp. 2d 596 (S.D.N.Y. 2010) (while the plaintiffs cannot seek copyright protection based upon the underlying raw financial data, database compilations and market research performance indices were sufficiently original under the Copyright Act because they do not contain simple mathematical averages, but are instead created through judgment being applied to disparate indicators; hot news misappropriation claim also survives dismissal, based upon allegations of the defendant's "constant and continuous unauthorized daily reproduction and multimedia redistribution").

test for hot news misappropriation outlined in *NBA*, and relied by the lower court and the parties as dicta, and instead focused on those "extra elements" that are necessary to avoid preemption. The appeals court rejected the plaintiffs' hot news claim because the defendant was not "free riding" by retaining a staff to summarize, disseminate, and report on the news of the plaintiffs' securities recommendations and attribute it to its source. In short, the court stated that: "The Firms are making the news; [the defendant], despite the Firms' understandable desire to protect their business model, is breaking it" and the defendant, having obtained news of a securities Recommendation, "is hardly selling the Recommendation as its own."

- **The Scranton Times, LP v. Wilkes-Barre Publishing Co. –** A newspaper's hot news misappropriation claim was preempted by the Copyright Act because the defendant's alleged misappropriation of non-copyrighted, time-sensitive obituaries from plaintiff's newspapers and website did not post a threat to the existence of plaintiff's publications.[33] The court denied the plaintiff's motion to remand, finding that the district court had subject matter jurisdiction over the plaintiff's misappropriation claim, among others, because it was preempted by the Copyright Act. While "narrow" hot news misappropriation claims will generally survive preemption, they must satisfy a five-factor test created by Second Circuit precedent. In this case, the court found that while the allegedly plagiarized obituaries were time-sensitive and that the defendant allegedly was "free-riding" off of the plaintiff's efforts in collecting them, the court ultimately concluded that such copying did not substantially threaten the quality of the plaintiff's publications or compromise the plaintiff's ability to continue the timely publication of the obituaries.

33. The Scranton Times, LP v. Wilkes-Barre Publishing Co., 90 U.S.P.Q.2d 1161 (M.D. Pa. Mar. 6, 2009). In further proceedings, the court ruled that the plaintiff's tortious interference, unfair competition, and unjust enrichment claims were preempted by the Copyright Act, but allowed the plaintiff's breach of contract and conversion claims to go forward. See The Scranton Times, LP v. Wilkes-Barre Publishing Co., 2009 WL 3100963 (M.D. Pa. Sept. 23, 2009). See also Silver v. Lavandeira, 2009 WL 513031 (S.D.N.Y. Feb. 26, 2009) (competing gossip website that allegedly copied facts and news items from the plaintiff's site did not likely commit copyright infringement because such facts and information were not protected by copyright and the defendant added his own distinctive tone making it a different expression); The Associated Press v. All Headline News Corp., 608 F. Supp. 2d 454 (S.D.N.Y. 2009).

- **Oracle America, Inc. v. Google, Inc.** – In 2014, the Federal Circuit overturned the District Court for the Northern District of California and held in favor of Oracle in a copyright infringement dispute against Google over the latter's use of packages of Oracle's computer source code (API packages) in its Android mobile operating system.[34] The Federal Circuit held that declaring code, structure, sequence and organization of the API Packages in question were entitled to copyright protection.[35] First, with respect to the source code, the court found that Oracle's API packages could be expressed in a number of ways, and therefore had not merged with the underlying source code.[36] The scope of copyrightability is evaluated at the time of the creation of the potentially protected expression. Also, the Federal Circuit noted that the relevant test for determining whether short phrases are copyrightable is not whether the phrases are short, but whether they are creative.[37] As such, because Oracle had "exercised creativity in the selection and arrangement" of the declaring code when creating the API Packages and wrote the relevant code, it contained protectable expression that is entitled to copyright protection. The Federal Circuit also rejected the District Court's notion that the API Packages cannot be copyrighted under the Act because it is a "system or method of operation."[38] Rather,

34. 750 F.3d 1339 (Fed. Cir. 2014); see Oracle America, Inc. v. Google Inc., 872 F. Supp. 2d 974 (N.D. Cal. 2012) ("*Copyrightability Decision*") (overturned decision).
35. Therefore, the notion that "Google replicated what was necessary to achieve a degree of interoperability with Java," is an errant prism through which to scrutinize interoperability claims. Copyrightability Decision, 872 F. Supp. 2d at 1000.
36. Another circuit has defined source code as the "spelled-out programs that humans can read." Lexmark Int'l, Inc v. Static Control Components, Inc., (387 F.3d 522).
37. Oracle America, Inc v. Google, Inc., 750 F.2d 1339 (Fed. Cir. 2014) (citing Soc'y of Holy Transfiguration Monastery, Inc. v. Gregory, 698 F.3d 29 (1st Cir. 2012)). At this point, the Federal Circuit enters into a tangential but nonetheless illuminating discussion of how the opening lines of Charles Dickens' A Tale of Two Cities: "It was the best of times, it was the worst of times," are "nothing but a string of short phrases." Nonetheless, "no one could contend that this portion of Dickens' works is unworthy of copyright protection because it can be broken into those shorter constituent components." Oracle America, 750 F.3d at 1363.
38. Copyrightability Decision, 872 F. Supp. 2d at 976-77 (citing 17 U.S.C. § 102(b)). In coming to this conclusion, the District court had relied on Lotus Development Corp. v. Borland International, Inc., 49 F.3d 807 (1st Cir. 1995), a case holding that a defendant who copied the menu command hierarchy and interface from a computer program designed to perform accounting functions electronically did not commit

the API packages could be copyrightable because the declaring code, structure and organization of the packages are both creative and original The court then turned to the question of "interoperability" in the context of claiming copyright. As background, aspects of software are not protected by copyright law if they are dictated by external factors, and therefore functional and not creative elements of the software. With respect to this issue, the Ninth Circuit has specifically recognized that: (1) Computer programs "contain many logical, structural, and visual display elements that are dictated by external factors such as compatibility requirements and industry demands." And (2) "[i]n some circumstances, even the exact set of commands used by the programmer is deemed functional rather than creative for the purposes of copyright." The interoperability question is "determined by the availability of choices to the plaintiff at the time the computer program was created, and therefore the relevant compatibility argument inquiry asks whether the plaintiff's choices were dictated by a need to ensure that its program worked with existing third-party programs." Ergo, as the District Court failed to realize, Google's decision to later make its Android system interoperable with Oracle's API Packages has "no bearing on whether the software [Oracle] created had any design limitations dictated by external factors."[39] Additionally, facts adduced by the presiding court noted that Google had specifically designed Android to *not* be compatible with Oracle's Java platform and the API Packages, a fact which illustrated that the API Packages and Android could not be "interoperable."

- **Apple, Inc. v. Psystar Corp.** – A computer maker that licenses copies of its operating system for use only on its own computers did not misuse its copyright and appropriately used its license to prevent infringement and control use of its copyrighted material.[40]

---

infringement because the command terms within the program were merely a method of operating the program itself. A number of other circuits have held that classifying a work as a "system" does not preclude copyright for the particular expression of that system. See, e.g., Am. Dental Ass'n v. Delta Dental Plans Ass'n, 126 F.3d 977 (7th Cir. 1997) ("[W]ord-processing software [is not] a system just because it has a command structure for producing paragraphs."); Toro Co. v. R & R Prods. Co., 787 F.2d 1208 (8th Cir. 1986) (rejecting the argument that a parts numbering system is not copyrightable because it is a "system") (internal quotations omitted).

39. 750 F.3d at 1371. Therefore, the notion that "Google replicated what was necessary to achieve a degree of interoperability with Java," is an errant prism through which to scrutinize interoperability claims. Copyrightability Decision, 872 F. Supp. 2d at 1000.
40. Apple, Inc. v. Psystar Corp., 658 F.3d 1150 (9th Cir. 2011).

The appeals court affirmed the lower court's grant of summary judgment in favor of Apple and its entry of a permanent injunction against Psystar's infringement of Apple's operating system through its sales of non-Apple computers that included Apple's operating system. The court rejected Psystar's argument that Apple had committed copyright misuse by requiring that all licensees of the Mac OS X operating system run their copies only on Apple computers. While the copyright misuse defense might prevent copyright holders from leveraging their limited monopoly to restrain development of competing products, the court found that the doctrine did not apply because Apple's licensing agreement merely restricted the use of Apple's own software to its own hardware and did not prevent others from developing their own computer or operating systems.

- **Vernor v. Autodesk, Inc.** – A software user is a licensee rather than an owner of a copy where the copyright owner (1) specifies that the user is granted a license; (2) significantly restricts the user's ability to transfer the software; and (3) imposes notable use restrictions.[41] The appeals court reversed the district's court grant of summary judgment in favor of the plaintiff- reseller on the copyright claim, concluding that an individual that resold used copies of software the original customer acquired pursuant to a software licensing agreement, which contained restrictions on use and transfer committed infringement, was not entitled to invoke the first sale doctrine or the essential step defense. This principal issue before the court was

41. Vernor v. Autodesk, Inc., 621 F.3d 1102 (9th Cir. 2010). See also Adobe Systems Inc. v. Hoops Enterprise LLC, 2012 WL 298732 (N.D. Cal. Feb. 1, 2012) (first sale doctrine is unavailable to eBay seller who resold OEM copies of Adobe software previously bundled with computer hardware distributed under a license that imposed significant transfer restrictions).

    The first sale doctrine also arises in the sale of gray market goods. See e.g., Microsoft Co. v. Intrax Group Inc., 2008 WL 4500703 (N.D. Cal. Oct. 6, 2008) (first sale doctrine only applies to copies legally made in the United States, or copies made abroad if the copies are sold in the U.S. by the copyright owner or with its authority); Microsoft v. Big Boy, 589 F. Supp. 2d 1308 (S.D. Fla. 2008) (first sale defense not applicable where software in question was manufactured and distributed overseas). See also Kirtsaeng v. John Wiley & Sons, Inc., 133 S.Ct. 1351 (2013) (first sale doctrine applies to copies of a copyrighted work lawfully made abroad and the statutory phrase "lawfully made under this title" did not impose a geographical limitation that prevents the doctrine from applying to foreign works made abroad with the copyright owner's permission; at a policy level, the Court noted that a contrary ruling would cause an adverse result in the marketplace because reliance on the first sale doctrine is deeply embedded in the practices of booksellers, libraries, museums, and retailers).

whether the software maker sold its software to its customers or licensed the copies to its customers. If the original customer that resold the software to the plaintiff "owned" its copies of the software, then both its sales to the plaintiff and the plaintiff's subsequent sales to third parties were noninfringing under the first sale doctrine; however, if the software maker only "licensed" the original customer to use copies of the software, then the original customer and the plaintiff's sales of those copies would not be protected by the first sale doctrine and would therefore infringe the software maker's exclusive distribution right under the Copyright Act. The court stated that the software maker retained title to the software and imposed significant restrictions, including, among other things, prohibitions on transfer, modification, translation, reverse engineering and usage outside of the Western Hemisphere. The software license agreement also provided for termination for unauthorized copying or usage. The court held that the software maker's customers were "licensees" of their copies of the software rather than "owners." Consequently, the court concluded that since the original customer of the software was not entitled to resell its copy to the plaintiff under the first sale doctrine and the plaintiff could not have passed ownership title to others, and as such, both the original customer and the plaintiff's sales infringed the software maker's copyright.

- **The Compliance Source, Inc. v. GreenPoint Mortgage Funding, Inc.** – A licensee that allowed its attorneys to access and use the licensed software to review and prepare real estate loan documents on its behalf may have breached the agreement because the license contained no provision that permitted the licensee to grant third-party access, whether or not such access would be on behalf of or for the benefit of the licensee.[42] The appeals court reversed the lower court's grant of summary judgment to the licensee and

42. The Compliance Source, Inc. v. GreenPoint Mortgage Funding, Inc., 624 F.3d 252 (5th Cir. 2010). See also Real View, LLC v. 20-20 Technologies, Inc., 811 F. Supp. 2d 553 (D. Mass. 2011) (court reduced a damage award against a company that illegally downloaded competitor's software and used it to develop competing, non-infringing software to an award of $4,200, the price of a license, and rejected as speculative or improper the argument that the plaintiff should have recovered damages for lost profits and price erosion based upon the initial illegal download). But see IBM Corp. v. BGC Partners, Inc., 2013 WL 1775367 (S.D.N.Y. Apr. 25, 2013) (court refused to grant licensor summary judgment on contract and copyright claims based upon unauthorized use of licensed software due to material issues of fact concerning what license governed the dispute, aggravated by the fact that the copy of the "bespoke" license that the licensee contends is governing was lost).

remanded the case. In reviewing the agreement, the court found that it expressly prohibited any use of the licensed technology not explicitly permitted by the agreement itself and other provisions allowing limited third-party access did not permit the type of input access that the licensee provided to its attorneys.

- **R.C. Olmstead, Inc. v. CU Interface, LLC** – A software maker's copyright infringement claim against a competitor is deficient when the software maker fails to show that any alleged similarities merely arose because both software programs were designed to address similar functions and evidence fails to identify any original, non-literal elements of the software copied by the competitor.[43] The appeals court affirmed the lower court's grant of summary judgment to the defendant on the copyright claim, concluding that the plaintiff's substantial similarity inquiry failed. The court found that the plaintiff did not even begin to provide the kind of abstraction-filtration-comparison analysis that would filter elements of its software that were original from elements that were unprotected and present to the court a compelling case of infringement.
- **Cincom Systems, Inc. v. Novelis Corp. –** A software licensee's series of mergers as part of an internal corporate restructuring, which, by law, transferred its software license rights to the surviving entity, violated the non-exclusive software license's express anti-assignment clause, resulting in liability for copyright infringement.[44] The court found that where state law would allow for the transfer of a copyright license absent express authorization, it must yield to the federal common law rule prohibiting such unauthorized transfers. The court concluded that only the original licensee was authorized under the agreement and if any other legal entity held the software

43. R.C. Olmstead, Inc. v. CU Interface, LLC, 606 F.3d 262 (6th Cir. 2010).
44. Cincom Systems, Inc. v. Novelis Corp., 581 F.3d 431 (6th Cir. 2009). See also HyperQuest Inc. v. N'Site Solutions Inc., 632 F.3d 377 (7th Cir. 2011) (software license did not clearly delineate exclusivity over at least one strand of the bundle of rights under Section 101 of the Copyright Act and thus licensee did not have the statutory authority to sue for copyright infringement; the fact that the license uses the phrase "exclusive license" or its equivalent from time to time is a factor, but not dispositive since it is the substance of the agreement, not the labels that it uses, that determines the difference between an exclusive and non-exclusive software license); QAD Inc. v. Conagra Foods Inc., 2011 WL 4964914 (C.D. Cal. Oct. 18, 2011) (licensor's dispute against company that acquired the original licensee allegedly in violation of software license's ambiguous assignment clause may proceed to arbitration).

license without the licensor's approval, then that entity had infringed the licensor's copyright because a transfer has occurred—regardless of whether the transfer took place by a particular act of the parties or by operation of state law.

- **Safety Mgmt. Sys., Inc. v. Safety Software Ltd. –** An exclusive licensing agent was not entitled to a preliminary injunction to require a software maker to deposit certain software in escrow with the plaintiff's counsel pursuant to the terms of a previous agreement because the licensing agent failed to show the prospect of imminent irreparable harm to the licensees or any immediate threat of the software maker's insolvency.[45] The court denied the plaintiff's motion for a preliminary injunction. The court found that to the extent that the licensing agent seeks to vindicate the rights of the licensees, the agent was not the proper party to raise such claims, particularly since none of the licensees appeared in this action or otherwise objected to the software maker having deposited the software into escrow under a different arrangement. The court also found that the action was a typical contract dispute and any harms could be redressed through monetary damages, as opposed to equitable relief.

Open Source Software

Generally speaking, open source software is software where the source code is made available to the public under a "public license," such that the source code can be read, modified and redistributed by users, subject to certain conditions. The open source approach is the conceptual and practical opposite of the idea of software as a "closed," proprietary product, distributed in the form of object code only, with the source code held privately by the owner. Much open source software is developed collaboratively by volunteer groups of programmers and typically is made available for download via the Internet. Many companies have chosen to incorporate open source software into their operations to achieve various goals such as cost savings, better control over software maintenance and modifications, or perhaps gain a competitive advantage. One example is the Linux operating system, one of the most well-known open source products. The Apache Web server product, which is estimated to power more

45. Safety Mgmt. Sys., Inc. v. Safety Software Ltd., 2010 WL 1837770 (S.D.N.Y. May 05, 2010).

than 70 percent of websites, is also an open source product, and the Mozilla Firefox Web browser is one of the more recent open source products to achieve wide public use.

One of the most frequently encountered open source licenses is promulgated by the Free Software Foundation—the GNU General Public License—commonly referred to as the GPL. The GPL permits the use of licensed software, even by commercial entities. However, conditions are placed on the modification and distribution of GPL-licensed code, namely, that if a work is based, in whole or in part, or contains or is derived from any part of GPL-licensed software, the new program must be licensed under the GPL and therefore must itself become open source. This potential impact of the GPL has been referred to as the "viral nature" of the GPL.

After an extensive drafting and comment period that began in 2006, the final draft of GPL Version 3 ("GPLv3") was released in June 2007. GPLv3 makes several substantial changes from the earlier versions, particularly pertaining to patent rights, which were drafted to address issues driven not only by the execution of law and technology but by certain developments in the conduct of players in the software industry. Although the GPL is one of the most prominent open source licenses, it is not the only one, as other entities have produced their own licenses, which may or may not be compatible with the latest version of the GPL. The GPL itself has spawned an official variant—the GNU Lesser General Public License (LGPL) to address some of the concerns raised by the "viral" provisions of the GPL. The LGPL is intended for use with software function and data libraries that are made to be linked to separate application programs to form executable programs. The LGPL allows the licensee to maintain the proprietary nature of the applications that are linked to the licensed library.

- **The SCO Group, Inc. v. Novell, Inc.** – This long-running litigation primarily involved a dispute between the plaintiff SCO and the defendant Novell regarding the scope of intellectual property and copyright rights in the UNIX software code allegedly retained by Novell following the sale of part of its UNIX business to a predecessor of the plaintiff in the mid-1990s.[46] The district court found that copyrights in the UNIX System V operating system were owned by Novell, entitling the company to dismissal of slander of title and related claims brought by SCO with respect

46. The SCO Group, Inc. v. Novell, Inc., 578 F.3d 1201 (10th Cir. 2009).

to statements made by Novell asserting its ownership of the copyrights. The lower court also ruled that under the terms of a 1995 transaction, the UNIX copyrights were excluded from the list of transferred assets and that Novell was entitled to royalties from certain licensing agreements entered into between SCO and Sun Microsystems and Microsoft in 2003. While the appeals court affirmed the award of royalties to Novell, it reversed the grant of summary judgment in favor of the defendant Novell regarding the copyrights in the UNIX code. After considering the evidence presented by both parties, the appeals court commented that the case involved "a complicated, multi-million dollar business transaction involving ambiguous language about which the parties offer dramatically different explanations," and as such, the dispute was "particularly ill-suited to summary judgment." The court took no position on which party ultimately owned the UNIX copyrights. The court remanded the case for trial, ruling that when conflicting evidence is presented such that the ambiguities in a contract could legitimately be resolved in favor of either party, it was a question of fact for the jury.

Following a trial, in March 2010, a jury ultimately concluded that two important Unix copyrights were owned by Novell. In further proceedings, the district court denied SCO's request for specific performance directing Novell to transfer the copyrights because the jury had determined that the parties' agreement did not transfer the copyrights from Novell to SCO, that it was not the intent of the parties to transfer ownership of the copyrights and the copyrights were not required for SCO to exercise its right with respect to the acquisition of UNIX technologies.[47] The court also granted Novell's motion for a declaratory judgment that it had authority under the agreement to direct SCO to waive claims against IBM, Sequent and other licensees or that Novell was entitled to waive such claims on SCO's behalf.

- **The Free Software Foundation, Inc. v. Cisco Systems, Inc.** – The parties settled their copyright dispute over the alleged unlicensed use and distribution of certain open source software programs.[48] According to the Complaint, the defendant allegedly

47. The SCO Group, Inc. v. Novell, Inc., 750 F. Supp. 2d 1050 (D. Utah 2010), *aff'd* 439 Fed. Appx. 688 (10th Cir. 2011).
48. The Free Software Foundation, Inc. v. Cisco Systems, Inc., No. 08-10764 (S.D.N.Y. Complaint filed Dec. 11, 2008). See also Software Freedom Conservancy Inc. v.

distributed to the public copies of its firmware containing the plaintiff's programs in its infringing products and via its website without providing complete and corresponding source code or an offer for source code as required by the GNU General Public License (GPL). Under the settlement agreement, the plaintiff agreed to dismiss its lawsuit and the defendant agreed to appoint a Free Software Director for its subsidiary Linksys to supervise compliance with the GPL and other open source licenses and make the source code for versions of the plaintiff's open source programs used with current Linksys products available on its website.

- **Jacobsen v. Katzer –** The terms of the open source Artistic License contain both covenants and conditions regarding users' modification and distribution rights in the downloadable software at issue that serve to limit the scope of the license and may form the basis of a cognizable copyright infringement claim.[49] The appeals court vacated the lower court's order and remanded for further factual findings regarding the plaintiff's motion for a preliminary injunction based upon copyright law. The court found that the Artistic License on its face created "clear and necessary" conditions by requiring users who modified or distributed the copyrighted software to make certain disclosures, and that the plaintiff had made out a prima facie case of copyright infringement based upon the defendant's incorporation of the software into one of its own commercial software packages. The court commented that the defendant acted outside the scope of the Artistic License when it modified and distributed the copyright materials without adhering to the stated license terms, and that compliance with such open source requirements - different than traditional licensing fees – were entitled to no less legal recognition.

  On remand, the district court denied the plaintiff's motion for a preliminary injunction because the plaintiff's claims of irreparable potential harm based upon defendant's alleged copyright

---

Best Buy Co., No. 09-10155 (S.D.N.Y. Complaint filed Dec. 14, 2009) (open source developer filed copyright infringement suit against various electronics retailers who allegedly distributed goods embedded with firmware that contained the plaintiff's open source software without complying with GPLv2). In further proceedings, the court granted the plaintiff's motion for a default judgment against an insolvent defendant-HDTV products maker who refused to participate in the litigation. See Software Freedom Conservancy Inc. v. Best Buy Co. Inc., No. 09-10155 (S.D.N.Y. July 27, 2010).

49. Jacobsen v. Katzer, 535 F.3d 1373 (Fed. Cir. 2008).

infringement (i.e., delays and inefficiency in development and time lost in the open source development cycle) were not supported by evidence of actual harm or any evidence of a real or immediate threat of imminent harm in the future.[50] In a further proceeding, the district court granted the plaintiff's motion for summary judgment on his copyright claim on liability only, rejecting the defendant's argument that the open source software project did not exhibit the requisite amount of creativity in the ordering and arrangement of data to qualify as copyrightable material.[51] The court also granted in part the plaintiff's motion for summary judgment on his DMCA claim. The court concluded that the defendant's actions of copying a program that contained software script that automatically added copyright notices and information regarding the software license and then removing the copyright information established elements of a DMCA Section 1202 removal of copyright management information claim, leaving issues of the defendant's requisite intent to be resolved at trial.

Digital Millennium Copyright Act

Congress enacted the Digital Millennium Copyright Act (DMCA)[52] to comply with international copyright treaties and to update domestic copyright law for the online world. The DMCA includes "anti-circumvention" provisions, which prohibit the circumvention of technological measures used by copyright owners to protect their works, as well as prohibitions against trafficking (that is, manufacturing and making available certain technologies or devices that are primarily designed to defeat technological protections that block unauthorized access). In conjunction, Congress also enacted Title II of the DMCA, the Online Copyright Infringement Liability Limitation Act (OCILLA),[53] to facilitate cooperation among Internet service providers and copyright owners over issues of infringement and provide greater certainty to service providers concerning their legal exposure for infringements.

50. Jacobsen v. Katzer, 609 F. Supp. 2d 925 (N.D. Cal. 2009).
51. Jacobsen v. Katzer, 2009 WL 4823021 (N.D. Cal. Dec. 10, 2009). Subsequently, the parties entered into settlement. The defendant will be subject to a permanent injunction, which among other things, prohibits the defendant from misusing the plaintiff's software and outlines the stipulated judgment of $100,000 in favor of the plaintiff. See Jacobsen v. Katzer, No. 06-01905 (N.D. Cal. Settlement Agreement filed Feb 18, 2010).
52. Pub. L. No. 105-304, 112 Stat. 2860 (1998).
53. 17 U.S.C. §512 (2003).

These statutory safe harbors[54] protect qualifying service providers from liability for all claims for monetary relief for direct, contributory and vicarious copyright infringement, leaving copyright owners with limited injunctive relief as set forth in 17 U.S.C. §512(j). Specifically, Section 512(c) is available to providers that store "information residing on systems or networks at the direction of users."[55] The safe harbors also include "notice and take down" provisions that require online service providers to remove or "takedown" any material posted by one of their subscribers upon receiving proper notification from a copyright owner that such material infringes the owner's copyright.

- **Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies (October 26, 2012)** — Every three years the Librarian of Congress is charged with determining whether there are any classes of works that will be subject to exemptions from the DMCA's prohibition against circumvention of technology that effectively controls access to a copyrighted work. Under the final rule, the following five classes of works will not be subject to the prohibition against circumventing access controls (17 U.S.C. § 1201(a)(1)):

  (1) Literary works distributed in ebook format when all existing ebook editions of the work contain access controls that prevent the enabling either of the book's read-aloud or other assistive function or of screen readers that render the text into a specialized format.

  (2) Circumvention of copy-protected DVDs to incorporate short portions of motion pictures into new works for the purpose of criticism or comment for educational uses by college and university professors and their students, documentary filmmaking, or noncommercial videos.

  (3) Computer programs that enable wireless telephone handsets to execute lawfully obtained software applications, where

54. 17 U.S.C. §512(a-d).
55. The "at the direction of the user" language in 17 U.S.C. § 512(c) is "clearly meant to cover more than mere electronic storage lockers." UMG Recordings, Inc. v. Shelter Capital Partners LLC, 718 F.3d 1006 (9th Cir. 2014). In that spirit, one federal court recently concluded that the fact that moderators had to approve infringing third party posts before such posts could become visible on a site does not disqualify the site from the safe harbor for infringement at the "direction of the user." See Marvix Photographs LLC v. LiveJournal Inc., No. SACV 13-00517-CRC(JPRx) (S.D. Cal. Sept. 19, 2014).

circumvention is accomplished for the sole purpose of enabling interoperability of such applications with computer programs on the telephone handset. Notably, this exemption permits the so-called practice of "jailbreaking," which some users of the iPhone and other smartphones engage in to download programs not authorized by their wireless carriers; however, the Librarian of Congress refused to expand the category of "wireless telephone handsets" to include the new generation of tablet computers.

(4) Computer programs, in the form of firmware or software, that enable a wireless telephone handset originally acquired from the operator of a wireless telecommunications network or retailer no later than January 26, 2013 ("legacy smartphones") to connect to a different wireless telecommunications network, if the operator of the wireless communications network to which the handset is locked has failed to unlock it within a reasonable period of time following a request by the owner of the wireless telephone handset, and when circumvention is initiated an individual consumer solely in order to connect to a different wireless telecommunications network, and such access to the network is authorized by the operator of the network.

(5) The circumvention of motion pictures and other audiovisual works contained on DVDs or delivered through online services to facilitate research and development of players capable of rendering captions and descriptive audio for persons who are blind, visually impaired or deaf.

- **Perfect 10, Inc. v. Amazon.com, Inc. –** This is a continuation[56] of the copyright litigation after remand from the Ninth Circuit, following its notable 2007 decision.[57] The defendant Amazon.com ("Amazon") moved to dismiss the remaining contributory copyright

56. Perfect 10, Inc. v. Amazon.com, Inc., 2009 WL 1334364 (C.D. Cal. May 12, 2009). See also Perfect 10 Inc. v. Google Inc., No. 04-9484 (C.D. Cal. July 26, 2010) (certain nonconforming DMCA notices not effective to provide notice of infringement, including notices sent to Google's webmaster as opposed to its DMCA agent and hard drives and DVDs ineffectually cross-referenced to a cover letter and list of infringing works; however, the court found that some spreadsheets, containing both incomplete and complete identifications of infringing works could have been effective under the DMCA).
57. Perfect 10, Inc. v. Amazon.com, Inc., 508 F.3d 1146 (9th Cir. 2007).

infringement claim based upon its displaying of allegedly infringing images in the search results of its A9 search engine. The plaintiff had sent takedown notices to the defendant Amazon, but not to its separate affiliate and co-defendant, A9. A9 moved for summary judgment on the ground that it was entitled to a safe harbor under 17 U.S.C. §512(c) because it was undisputed that the plaintiff sent takedown notices to Amazon, instead of to A9 (and only sent notices to A9 after the commencement of the suit). The plaintiff argued that the defendants had actual knowledge of the notices and otherwise should be estopped from claiming the DMCA safe harbor because it failed to comply with certain requirements of the statute. The court held that A9 was entitled to a finding that it is entitled to a safe harbor under § 512(c) and summary judgment as to contributory copyright infringement.

The court found that the plaintiff cited no authority that would require one ISP, by virtue of its ownership or hosting of another ISP, to pass along a DMCA notice, where the two ISPs are distinct corporate entities and, more importantly, have each properly designated a copyright agent to receive DMCA takedown notices. The court rejected the plaintiff's argument that Amazon's website Conditions of Use instructed copyright owners to send DMCA notices regarding its affiliates directly to Amazon, finding that nowhere in those Conditions of Use does Amazon purport to include A9 among its "affiliates." The court also stated that Amazon's filing with the Copyright Office identifying the subsidiary entities for which Amazon's copyright agent would accept complaints did not include A9. Moreover, the court commented that A9's website contained its own Conditions of Use, which the plaintiff inexplicably failed to digest. The court also rejected the plaintiff's argument that A9 did not substantially comply with the designation requirements of the statute because A9 provided not an email address for its copyright agent, but a URL for the online complaint form, a distinction that the court found "inconsequential."

- **MDY Industries, LLC v. Blizzard Entertainment, Inc. –** A video game's terms of use prohibiting bots and the installation of unauthorized third-party "cheat" software were covenants rather than copyright-enforceable conditions and a user who violates such covenants may be liable for breach of contract but not

copyright infringement.[58] The court reversed the lower court's judgment finding the plaintiff liable for secondary copyright infringement for selling "cheat" software to users of Blizzard's video game. The court concluded that for a licensee's violation of a contract to constitute copyright infringement, there must be a nexus between the condition and the licensor's exclusive rights of copyright, and that, in this case, the use of the "cheat" software did not alter or copy the game software or otherwise infringe any of video game maker's exclusive copyright rights. The court commented that: "Were we to hold otherwise, Blizzard — or any software copyright holder — could designate any disfavored conduct during software use as copyright infringement, by purporting to condition the license on the player's abstention from the disfavored conduct. The rationale would be that because the conduct occurs while the player's computer is copying the software code into RAM in order for it to run, the violation is copyright infringement. This would allow software copyright owners far greater rights than Congress has generally conferred on copyright owners." However, the appeals court affirmed the lower court's ruling that Blizzard was entitled to a permanent injunction against the plaintiff's continued sale, distribution, and servicing of the "cheat" software based on violations of DMCA § 1201(a)(2), which prohibits trafficking in technology that circumvents a technological measure that "effectively controls access" to a copyrighted work, in this case, the live-action elements of the video game. One of the notable issues raised by the appeal was whether certain provisions of DMCA § 1201 prohibit circumvention of access

58. MDY Industries, LLC v. Blizzard Entertainment, Inc., 629 F.3d 928 (9th Cir. 2010). In a related copyright issue, the court held that the game users (and the plaintiff) could not claim any defenses under Section 117 of the Copyright Act as "owner" of a copy of software. Following its precedent in Vernor v. Autodesk, 621 F.3d 1102 (9th Cir. 2010), the appeals court ruled that game players were mere licensees of Blizzard's game software because Blizzard reserved title in the software and granted players a non-exclusive, limited license with significant transfer and use provisions. See also Avaya Inc. v. Telecom Labs Inc., No. 06-2490 (D.N.J. Nov. 4, 2011) (unpublished) (court declined to impose a "nexus" requirement, finding that nothing in DMCA §1201 requires that there be a reasonable relationship between circumvention and copyright infringement; regardless of how a login/password combination is obtained, such "unauthorized use of a technological measure without the authority of the copyright owner" does not fall within the definition of circumvention and therefore does not constitute a violation of § 1201(a)(1)).

controls when access does not constitute copyright infringement. Declining to follow a line of cases from the Federal Circuit, which required§ 1201(a) plaintiffs to demonstrate that the circumventing technology infringes or facilitates infringement of the plaintiff's copyright (a so-called "infringement nexus requirement"), the Ninth Circuit held that a fair reading of the statute indicated that Congress created "a distinct anti-circumvention right under § 1201(a) without an infringement nexus requirement." The court concluded that Blizzard had established all of the six elements of a § 1201(a)(2) anti-circumvention trafficking violation and it affirmed the district court's entry of a permanent injunction against the plaintiff to prevent future § 1201(a)(2) violations.

As the popularity of Web video continues to grow, so too does the potential for contributory copyright infringement on popular video-sharing websites. These websites invariably become venues for infringing behavior, not necessarily due to the site's architecture or purpose, but simply due to the sheer number of users uploading new videos daily. Consequently, content owners continue to contend that such websites must take a greater role in stemming their users' infringement. In response, website owners have countered that they need only follow the dictates outlined by the DMCA safe harbors that immunize qualifying service providers from copyright liability. Thus, both sides continue to dispute what it means to be compliant with the DMCA and who should bear the ultimate responsibility, the site owner or the content owner, for policing video-sharing sites for infringing content.

- **Viacom Int'l, Inc. v. YouTube, Inc. –** Actual knowledge or awareness of facts or circumstances that indicate specific and identifiable instances of infringement will disqualify an online storage provider from the DMCA safe harbor, 17 U.S.C. §512(c).[59] General knowledge that copyright infringement is occurring does not impose a duty on the service provider under the DMCA safe harbor to monitor or search its service for infringements. In a

59. Viacom Int'l, Inc., v. YouTube, Inc., 676 F.3d 19 (2d Cir. 2012). See also Obodai v. Demand Media Inc., 2012 WL 2189740 (S.D.N.Y. June 13, 2012), *aff'd* 522 Fed. Appx. 41 (2d Cir. 2013) (website that was not served with takedown notices but removed plaintiff's copyrighted content after being served with a complaint deemed protected by DMCA safe harbor; court rejected plaintiff's argument that site-traffic monitoring and third-party ads triggered alongside the infringing content could constitute control over the material).

notable decision, the appeals court affirmed the lower court's interpretation of the DMCA safe harbor with respect to the "specificity" requirement of §512(c)(1)(A), affirming that the nature of the removal obligation under the statute contemplates "knowledge or awareness of specific infringing material" and rejecting the plaintiff's argument that a site should take "commercially reasonable steps" in response to a generalized awareness of infringement. However, the appeals court reversed the lower court's grant of summary judgment in favor of the video sharing website, ruling that summary judgment was premature given material issues of fact surrounding the service provider's knowledge or awareness of specific instances of infringement. The appeals court first clarified the actual and "red flag" knowledge standards under the statute: "The difference between actual and red flag knowledge is thus not between specific and generalized knowledge, but instead between a subjective and an objective standard. [T]he actual knowledge provision turns on whether the provider actually or '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 person."[60] Regarding the claims that the defendant knew that it was hosting infringing content, the court found material issues of fact regarding the site's knowledge or awareness of specific instances of infringement, specifically several internal emails that suggested employees had actual or red flag knowledge that the site was hosting "clearly infringing" and "blatantly illegal" copyrighted material.[61] On an issue of first impression, the court also considered the application of the common law willful blindness doctrine in the DMCA context,

60. See also Capitol Records, Inc. v. MP3tunes, LLC, –- F. Supp. 3d — (S.D.N.Y. 2014) (overturning jury verdict of liability on theories of red flag knowledge and willful blindness because defendant did not have specific knowledge, must less general knowledge, of infringing content on its website, therefore to impute liability would force the defendant to take commercially reasonable steps to research and identify other instances of infringing content).
61. See also Capitol Records, LLC v. Vimeo, LLC, 972 F. Supp. 2d 537 (S.D.N.Y. 2013) (when site employees have never viewed allegedly infringing videos posted on video-sharing site, the site could not be aware of facts or circumstances that would engender "red flag" knowledge of infringement, and therefore could avail itself of DMCA safe harbor with respect to these videos; however, videos with copyrighted material that contained comments from site employees or were "buried" or "liked" by site employees imputed "red flag" knowledge to the site).

concluding that the doctrine may be applied, in appropriate circumstances, to demonstrate knowledge or awareness of specific instances of infringement under the DMCA. The court remanded the issue to the lower court to determine whether the defendant made a "deliberate effort to avoid guilty knowledge." Last, the court considered the DMCA safe harbor's so-called "control and benefit" requirement, that an eligible service provider must "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." The appeals court reversed the lower court's holding that "control and benefit" requires specific knowledge of infringing activity. The court refused to equate "control and benefit" with vicarious liability (which would conceivably trigger an obligation based upon the premise that the mere "ability to block infringers' access to a particular environment for any reason whatsoever is evidence of the right and ability to supervise), yet still held that the "right and ability to control" infringing activity under § 512(c)(1)(B) "requires something more than the ability to remove or block access to materials posted on a service provider's website." The definition of "something more" was left to the lower court to consider.

On remand, the district court considered several issues, including: (1) whether YouTube had knowledge or awareness of any specific infringement concerning the clips in suit; (2) whether YouTube was willfully blind to specific infringements; and (3) whether YouTube had the "right and ability to control" infringing activity within the meaning of §512 (c)(1)(B).[62] As to the first issue, the court concluded that neither side possessed sufficient evidence that would allow a clip-by-clip assessment of actual knowledge. The court noted: "If…neither side can determine the presence or absence specific infringements because of the volume of material, that merely demonstrates the wisdom of the legislative requirement that …the owner of the copyright…identifies the infringement by giving the service provider notice." The court further noted that "the burden of showing that YouTube knew or was aware of the specific infringements of the works in suit cannot be shifted to YouTube to disprove." On the second issue, the court found that although YouTube may have known of the general presence of infringing material on its service, the DMCA does not require the

62. See Viacom Int'l, Inc., v. YouTube, Inc., 940 F. Supp. 2d 110 (S.D.N.Y. 2013).

provider to affirmatively seek facts indicating infringing activities and as such, there was no evidence of willful blindness to specific infringements regarding the clips in suit. Concerning the "right and ability to control" issue, the court stated that the concept generally means that a provider, even without knowledge of specific infringing activity, might so influence or participate in that activity, while gaining a financial benefit from it, as to lose the safe harbor, such as by high levels of control over the activities of users or purposeful conduct regarding infringing activities. The court reiterated, however, that "knowledge of the prevalence of infringing activity, and welcoming it, does not itself forfeit the safe harbor. To forfeit that, the provider must influence or participate in the infringement." Concerning the "right and ability to control" issue, the court ruled that YouTube did not have the right and ability to control infringing activity, stating that beyond operating its automated service and monitoring its site for certain unwanted types of content, YouTube did not induce its users to submit infringing content, offer instructions of what content to upload, steer users to infringing videos, or otherwise interact with users to a point where it could be said that it participated in their infringing activities.

- **Flava Works, Inc. v. Gunter –** A social video bookmarking website that allowed users to embed, share and store inline links to videos is not likely liable for contributory copyright infringement because, among other things, there was no evidence that the site contributed to the decisions of the original users who uploaded plaintiff's videos to the Internet where they then would be available to be bookmarked on the defendant's site.[63] The appeals court vacated the lower court's entry of a preliminary injunction preventing the posting of links and embedded videos containing plaintiff's copyrighted content. The court commented that the direct infringer was the customer of the plaintiff who copied its copyrighted video by uploading it to the Internet, but that someone who clicked on one of the links to watch a copyrighted video for free without making a copy is "no more a copyright infringer than if he had snuck into a movie theater and watched a copyrighted movie without buying a ticket." The court stressed that the infringers were the uploaders of copyrighted work and there was no evidence that the defendant encouraged them, which would make

63. Flava Works Inc. v. Gunter, 689 F.3d 754 (7th Cir. 2012).

it a contributory infringer. The court noted that the plaintiff may be entitled to additional preliminary injunctive relief if it can show, as it has not shown yet, that the defendant's service really does contribute significantly to infringement of its copyrights.

- **UMG Recordings, Inc. v. Veoh Networks, Inc. –** Software functions and automated file conversions directed toward facilitating access to video materials stored at the direction of users fall within the scope of DMCA §512(c) because the safe harbor extends to functions other than mere storage and applies to infringement of copyright by reason of the storage at the direction of a user.[64]

  In further proceedings, the court granted summary judgment in favor of the defendant on the plaintiff's copyright claims.[65] In light of the principles articulated in the Ninth Circuit's *CCBill* opinion[66] that the burden is on the copyright holder to provide notice of allegedly infringing material, and that it takes willful ignorance of readily apparent infringement to find a "red flag," the court found that the defendant had provided substantial evidence that it fulfilled the requirements of the DMCA section 512(c)(1)(A) safe harbor. The court rejected the plaintiff's argument that the defendant's video sharing website should have sought out actual knowledge of infringing videos by searching its system for all videos by the artists identified in notices sent on its behalf by an industry group, finding that a valid takedown notice must identify the copyrighted works claimed to have been infringed, not merely list individual artists. Regarding notice of infringement, the court found that while it is "common knowledge" that most websites that allow users to contribute material invariably host infringing items, such general awareness is not enough to raise a "red flag" under the statute. Lastly, the court rejected the plaintiff's argument that the DMCA imposes an obligation on a service provider to implement filtering technology, "let alone technology from the copyright holder's preferred vendor or on the copyright holder's desired timeline."

64. UMG Recordings, Inc. v. Veoh Networks, Inc., 620 F. Supp. 2d 1081 (C.D. Cal. 2008).
65. UMG Recordings, Inc. v. Veoh Networks, Inc., 665 F. Supp. 2d 1099 (C.D. Cal. 2009).
66. Perfect 10, Inc. v. CCBill LLC, 488 F.3d 1102 (9th Cir. 2007).

On appeal, the Ninth Circuit affirmed the district court's determination on summary judgment that Veoh was entitled to § 512(c) safe harbor protection.[67] Interestingly, the appeals court rejected the plaintiff's argument that since the sharing site hosted a category of copyrightable content — music —it must have known this content was infringing. The court concluded that merely hosting a category of copyrightable content, such as music videos, with the general knowledge that one's services could be used to share infringing material, is insufficient to meet the actual knowledge requirement under §512(c)(1)(A)(i). Concerning "red flag" knowledge, the court held that general knowledge that it hosted copyrightable material and that its services could be used for infringement was insufficient to constitute a red flag, though, "a service provider cannot willfully bury its head in the sand to avoid obtaining such specific knowledge." The court added: "the DMCA recognizes that service providers who do not locate and remove infringing materials they do not specifically know of should not suffer the loss of safe harbor protection." The court also stated that the following acts could not constitute a "red flag": (1) tagging of content as "music videos"; (2) purchasing recording artist names as search engine advertising keywords; (3) informal emails sent by the copyright holder to the service provider about specific works being infringed, which, the service provider acted upon, but should have been sent as a proper DMCA takedown notice [The court noted that if such a 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 because it specified particular infringing material].

- **Columbia Pictures Industries, Inc. v. Fung** – A BitTorrent file-sharing website that facilitated and encouraged users' infringement of copyrighted files and whose marketing efforts encouraged users to copy and distribute copyrighted music and movie files and whose business model depended on massive infringement is liable for

67. UMG Recordings, Inc. v. Shelter Capital Partners LLC, 718 F.3d 1006 (9th Cir. 2013). See also IO Group, Inc. v. Veoh Networks, Inc., 586 F. Supp. 2d 1132 (N.D. Cal. 2008) (video sharing site that actively enforces its user policy, acts expeditiously to remove infringing material, and seeks to prevent the same infringing content from being re-posted qualifies for the DMCA 512(c) safe harbor; DMCA does not require service providers to track users in a particular way (e.g., verification of users' IP addresses) or affirmatively police users for evidence of repeat infringement).

active inducement of copyright infringement.[68] The court granted summary judgment to the copyright holders, finding ample evidence that the defendant offered his services with the object of encouragement users of its service to upload infringing BitTorrent files containing copyrighted content. The court reasoned that inducement liability is not limited to those who distribute a "device" and one can infringe a copyright through culpable actions resulting in the impermissible reproduction of copyrighted expression, whether those actions involve making available a device or product or providing some service used in accomplishing the infringement. Regarding the DMCA safe harbor, the court held that the defendant had "red flag" knowledge of a broad range of infringing activity for reasons independent of any takedown notifications, and therefore was ineligible for the § 512(c) safe harbor. Interestingly, the court rejected the argument that inducement liability is inherently incompatible with protection under the safe harbors: "potential liability for contributory and vicarious infringement [does not] render[] the [DMCA] inapplicable per se."

- **Capitol Records, Inc. v. MP3Tunes –** An online music storage locker service that allowed users to locate and download for storage free song files on the internet was entitled to the DMCA safe harbor because of its compliance with statutory requirements and takedown notices that identified specific links to infringing content, but did not qualify for safe harbor protection for song files "sideloaded" from links identified as infringing by proper takedown notices that the site failed to remove from user lockers.[69] The court, among other things, granted the plaintiff's motion for summary judgment on its contributory copyright infringement claim for songs noticed in takedown notices and not removed from user lockers, but granted the defendant's motion for summary judgment on its defense under the DMCA safe harbors with respect to other claims. The court rejected the plaintiff's argument that the court should construe the terms "free," "mp3," or "file-sharing"

68. Columbia Pictures Industries, Inc. v. Fung**,** 710 F.3d 1020 (9th Cir. 2013).
69. Capitol Records, Inc. v. MP3Tunes, LLC, 821 F. Supp. 2d 627 (S.D.N.Y. 2011) (amended opinion). See also UMG Recordings Inc. v. Escape Media Group Inc., 107 A.D.3d 51 (N.Y. App. Div. 2013) (DMCA safe harbors do not provide a defense to service providers facing common law copyright infringement claims related to pre-1972 music recordings because Section 301(c) forbids the Copyright Act from "annull[ing]" or limit[ing]" the common-law rights and remedies of owners of such works).

as tantamount to "red flag" knowledge of infringement when such terms are used in domain names of sites that offer free music. The court stated that those terms are "ubiquitous among legitimate sites offering legitimate services" and that as part of viral marketing campaigns, music companies regularly distribute works on the internet for free, such that users and providers have no way of knowing for sure whether free songs on the internet are unauthorized. Moreover, the court stated that takedown notices that do not substantially comply with the DMCA or that simply give representative lists of copyrighted works that should be removed do not establish actual or "red flag" knowledge of infringement.

In further proceedings, the court granted the service provider's motion for summary judgment. The court rejected the plaintiff's direct infringement claims, concluding that the provider's copying of the plaintiff's images for product simulations and other similar displays is not the type of volitional conduct sufficient for direct liability. The court also found that the defendant was protected by the DMCA safe harbor. The court found that the defendant could not be held liable for its failure to remove images for which the plaintiff failed to provide proper notice, rejecting the "active enforcement" argument that one takedown notice should apply to all instances of infringement appearing on the website: "Notices that do not identify the specific location of the alleged infringement are not sufficient to confer 'actual knowledge' on the service provider."

- **Lenz v. Universal Music Corp. –** To comply with the §512(c) safe harbor's requirement that a DMCA takedown notice be backed with "a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law," a copyright owner must evaluate whether the material is protected under the fair use doctrine of the Copyright Act.[70]

70. Lenz v. Universal Music Corp., 572 F .Supp. 2d 1150 (N.D. Cal. 2008). But see Third Education Group, Inc. v. Phelps, 675 F. Supp. 2d 916 (E.D. Wis. 2009) (plaintiff failed to demonstrate that defendant lacked a good faith belief that he owned the copyright when he sent a DMCA takedown notice to the plaintiff, particularly since determining ownership of the website material in question required resolution of complex legal questions regarding state law). See also Amaretto Ranch Breedables LLC v. Ozimals Inc., No. 10-5696 (N.D. Cal. Apr. 22, 2011) (a claim under DMCA § 512(f) for filing false takedown notices with a service provider is not viable where no takedown of the copyrighted material occurs; a § 512(f) plaintiff's damages must be proximately caused by the misrepresentation to the

The court denied the defendant's motion to dismiss. The court found that an allegation that a copyright owner acted in bad faith by issuing a takedown notice without proper consideration of the fair use doctrine is sufficient to state a claim for misrepresentation under §512(f) of the DMCA. The court commented that while some evaluations of fair use "will be more complicated than others," in the majority of cases, "a consideration of fair use prior to issuing a takedown notice will not be so complicated as to jeopardize a copyright owner's ability to respond rapidly to potential infringements."

In a further proceeding, the court granted the plaintiff's motion for summary judgment on several of the defendant's affirmative defenses, including that the plaintiff suffered no damages, finding that the plaintiff incurred at least some damage under the statute.[71] The court initially determined what types of damages, as a matter of law, were compensable under §512(f) and found that the statute's allowance for the recovery of "any damages" suggested that recovery was available even if it do not amount to the substantial economic damages. However, the court held that a § 512(f) plaintiff's damages must be proximately caused by the misrepresentation to the service provider and the service provider's reliance on the misrepresentation. Accordingly, the court stated

---

service provider and the service provider's reliance on the misrepresentation). In further proceedings, the court found that interference with contract and other related claims and other state law claims based on allegedly false takedown notifications were preempted by the DMCA, which is the sole remedy for a recipient of such a notice. Amaretto Ranch Breedables LLC v. Ozimals Inc., 2011 WL 2690437 (N.D. Cal. July 8, 2011).

71. See Lenz v. Universal Music Corp., 2010 WL 702466 (N.D. Cal. Feb. 25. 2010).; see also Crossfit, Inc. v. Alvies, 2014 WL 251760 (N.D. Cal. Jan. 22, 2014) (knowingly sending a DMCA takedown notice referencing a violating trademark instead of a violating copyright could constitute a material misrepresentation sufficient to incur liability under 17 U.S.C. § 512(f)); Ouellette v. Viacom Int'l, Inc., 2012 WL 1435703 (D. Mont. April 25, 2012) (claim under 17 U.S.C. § 512(f) for wrongful DMCA takedown notice dismissed; liability for a misrepresentation under § 512(f) may be imposed only upon a showing of a copyright owner's subjective bad faith, where the owner makes "a knowing misrepresentation," and will not be imposed only upon "an unknowing mistake," even if the copyright owner acted unreasonably in making the mistake); Tuteur v. Crosley-Corcoran, — F. Supp. 2d — (D. Mass. 2013) (no requirement in the DMCA that a notice-giver inform the service provider of an infringer's possible affirmative defenses, only that she affirm her good faith belief that the copyrighted material is being used without her permission).

that while any fees incurred for work in responding to the takedown notice and prior to the institution of suit under §512(f) are recoverable under that provision, recovery of any other costs and fees subsequent to litigation would be governed by §505, the Copyright Act's attorney's fee provision. In dicta, the court commented on the effect of the ruling: "[I]t may be that the combination of the subjective bad faith standard[72] and the proximate causation requirements will lead many potential §512(f) plaintiffs to refrain from filing suit unless they have suffered substantial economic harm or other significant inconvenience."

Trade Secret and Other Misappropriation

State trade secret law can help to secure proprietary protection for confidential formulas and processes and much of the valuable and confidential information that may be shared between the parties developing a new product. Trade secret protection can also help to secure proprietary, secret company information from being disclosed or misused by departing employees. Trade secret information can include many types of competitively valuable secret information, including financial information and technical data and design specifications and software.

- **Silvaco Data Systems v. Intel Corp.** – A business customer cannot be liable for misappropriation of source code based upon the act of executing software in object code form that it had purchased from another software company and thereafter learning that the seller had been accused of incorporating stolen source code in the product.[73] The state appellate court affirmed the lower court's grant of summary judgment to the defendant-customer on the plaintiff's trade secret misappropriation claim. The court ruled that there was no basis for finding that the defendant ever "acquired" the source code constituting the trade secrets, as required under the California trade secrets statute, particularly since the defendant initially purchased the software without any inkling that the seller might have developed the software in a questionable manner. The court commented that the statute's choice of the term "acquire" as opposed to "receive" suggested that inadvertently coming into possession of a trade secret will

72. See Rossi v. Motion Picture Ass'n of Am. Inc., 391 F.3d 1000 (9th Cir. 2004).
73. Silvaco Data Systems v. Intel Corp., 184 Cal. App. 4th 210 (Cal. Ct. App. 2010).

not constitute acquisition, such that one who passively receives a trade secret, but neither discloses nor uses it, would not be guilty of misappropriation. The court also stated that "strong considerations of public policy" reinforced its holding: if the act of loading finished software constituted a use of the source code from which it was compiled, "then every purchaser of software would be exposed to liability if it were later alleged that the software was based in part upon purloined source code."

- **Nationwide Mutual Insurance Co. v. Mortensen** – A computer database containing policyholder information is not a protectable trade secret under Connecticut law because similar information existed in physical policyholder files that were readily available.[74] The appeals court affirmed the lower court's dismissal of the plaintiff's trade secret claims against departing employees who allegedly shared policyholder information with competitors. The court stated that merely because the customer information was stored in a better-protected, digital, password-protected format than the physical folders does not elevate the data to trade secret status. The court commented that "it is not the medium that matters here, but whether the information itself was adequately protected – and [in this case] it was not."
- **Aqua Connect, Inc. v. Code Rebel, LLC –** A breach of a clause in a form EULA cannot convert an act of reverse engineering into trade secret misappropriation based upon an purported act of "improper means."[75] The court dismissed the plaintiff's trade secret claim, commenting that the defendant's alleged breach of the EULA might form a cognizable contract claim. The court refused to read a "duty to maintain secrecy" into a form software license

74. Nationwide Mutual Insurance Co. v. Mortensen, 606 F.3d 22 (2d Cir. 2010). See also Tewari De-Ox Systems, Inc. v. Mountain States/Rosen, L.L.C., 637 F.3d 604 (5th Cir. 2011) (proprietary method was not a trade secret because the owner had previously disclosed it in a prior patent application); Scienton Technologies, Inc. v. Computer Associates Int'l Inc., 2013 WL 1856653 (E.D.N.Y. May 1, 2013) (plaintiffs' purported trade secret –the idea or concept of combining certain program functionalities and not the source code or technical details regarding how those different programs would interact with one another– was not entitled to protection; court noted that the secrecy of plaintiffs' "concept" would have necessarily been lost once the product was placed on the market). But see Decision Insights, Inc. v. Sentia Grp., Inc., 311 Fed. Appx. 586 (4th Cir. 2011) (software compilation of publicly-known algorithms that was not generally known or readily ascertainable by proper means could be trade secret).
75. Aqua Connect, Inc. v. Code Rebel, LLC, No. 11-5764 (C.D. Cal. Feb. 13, 2012).

agreement and found that under California law, reverse engineering must be combined with some other improper action to form the basis of a trade secret misappropriation claim

- **Simplexgrinnell LP v. Integrated Systems & Power, Inc. –** A licensee's unauthorized use of a software key that facilitated multiple functions of the licensed software was deemed trade secret misappropriation, warranting injunctive relief.[76]
- **KnowledgePlex, Inc. v. Placebase, Inc. –** A company may bring a trade secret misappropriation against a software development subcontractor that, under a work for hire arrangement, handled a complex, confidential project based upon allegations that the subcontractor developed its own similar product in dramatically less time, at an inferior cost, and with fewer resources, suggesting that the subcontractor could only have copied the plaintiff's confidential code.[77]

ONLINE DEFAMATION

Long before the digital age, the law wrestled with balancing the competing interests in compensating parties for attacks upon their reputations and protecting the First Amendment rights of journalists and individuals. Today, however, the Internet makes it easy to disseminate information and ideas anonymously, offering bloggers and users who post comments

76. Simplexgrinnell LP v. Integrated Systems & Power, Inc., 642 F. Supp. 2d 167 (S.D.N.Y. 2009). See also Shutterfly Inc. v. ForeverArts, Inc., 2012 WL 2911887 (N.D. Cal. July 13, 2012) (in a copyright and trade secret case involving misappropriation of proprietary source code by former employee for use in a competing venture in China, court issued TRO prohibiting defendant from destroying evidence). But see R.C. Olmstead, Inc. v. CU Interface, LLC, 606 F.3d 262 (6th Cir. 2010) (user interface product was not a trade secret because the owner did not take reasonable steps to maintain its secrecy; owner's agreement with licensee did not contain any confidentiality provisions preventing third parties from viewing the interface, and that the agreement expressly contemplated that the licensee would use a third-party personal computer support firm to assist with support and to provide the terminal emulation software).
77. KnowledgePlex, Inc. v. Placebase, Inc., 2008 WL 5245484 (N.D. Cal. Dec. 17, 2008). See also Contour Design, Inc. v. Chance Mold Steel Co., 2010 WL 174315 (D. N.H. Jan. 14, 2010) (concept for a computer mouse design that was not yet perfected or manufactured could be a protectable trade secret). But see KEMA, Inc. v. Koperwhats, 96 U.S.P.Q.2d 1787 (N.D. Cal. 2010) (no misappropriation due to failure to undertake reasonable efforts to maintain the secrecy of the trade secret where programmer admitted that he provided the source code to defendant without any confidentiality agreement or other restriction).

on websites the ability to express themselves behind cloaked identities, sometimes in an defamatory manner. Indeed, the rise of online interactivity has raised multiple issues for civil litigants concerning the identification of anonymous parties that have allegedly posted defamatory statements on the Internet. For the most part, websites and providers of interactive services are immune from third-party liability under §230 of the Communications Decency Act (CDA) for the mere posting of user-generated content. However, the CDA offers no immunity to individuals who post online defamatory statements, and therefore, if these individuals can be identified, they may be held liable under applicable state laws.

- **Seaton v. TripAdvisor, LLC** – An online travel ratings site that created a Top Ten Dirtiest Hotels list based upon user comments and data is not liable for defamation because a reasonable person could not understand the list in question as an assertion of fact instead of merely "unverifiable rhetorical hyperbole" and the aggregated opinion of the site's millions of online users.[78] The court granted the defendant's motion to dismiss. The court concluded that the plaintiff failed to plead any facts that showed the defendant made a statement of fact, or a statement of opinion that it intended readers to believe was based on facts. The court also noted that although the site's method of arriving at its conclusions (i.e., unverified online user reviews) was "a poor evaluative metric," it was not a "system sufficiently erroneous so as to be labeled 'defamatory' under the legal meaning of the term."
- **SPEECH Act** – In 2010, Congress passed the SPEECH Act, which, among other things, prohibits a domestic court from recognizing a foreign judgment for defamation unless the defamation law applied in the foreign court's adjudication provided at least as much protection for freedom of speech as would be provided by the First Amendment.[79] The Act also provides that any U.S. person, against whom a foreign judgment is entered on the basis of published speech, may bring an action in district court for a declaration that the foreign

78. Seaton v. TripAdvisor, LLC, 2012 WL 3637394 (E.D. Tenn. Aug. 22, 2012). See also Rahbar v. Batoon, 2012 WL 4883236 (Cal. Ct. App. Oct. 16, 2012) (unpublished) (former patient granted attorney's fees after successful anti-SLAPP motion against health care provider's defamation suit over online comments); Perez v. Dietz Development, LLC, 2012 WL 6761997 (Va. Dec. 28, 2012) (preliminary injunction ordering Yelp reviewer to edit negative posting about plaintiff-contractor and not post similar remarks on other sites was vacated since the plaintiff may seek an adequate remedy under law).
79. Pub. L. 111-223, codified at 28 U.S.C. §§ 4101-4105 (2010).

judgment is repugnant to the Constitution. Domestic courts are also prohibited from enforcing a foreign judgment for defamation against the provider of an interactive computer service, as defined in CDA Section 230, unless the domestic court determines that the judgment would be consistent with Section 230 if the user-generated content that is the subject of such foreign judgment had been provided in the United States.

- **Sedersten v. Taylor** – A website privacy policy that grants the site the right to disclose user information "in any way and for any purpose" did not act as waiver of the First Amendment rights of the anonymous non-party poster when nothing on the face of the privacy policy hinted that users may be waiving constitutional rights by posting comments to the site.[80] The court denied the plaintiff's motion to compel the identity of the anonymous website poster. The court also found that the plaintiff failed to make an adequate showing that this was an exceptional case that warranted disclosure of an anonymous non-party speaker's identity, particularly given the political nature of the poster's online speech.
- **Too Much Media LLC v. Hale** – A self-proclaimed "information exchange" website operator who allegedly posted defamatory comments on Internet bulletin boards and forums for the purpose of informing the public of the plaintiff's unlawful dealings may not refuse to divulge her sources by claiming protection under the New Jersey Shield Law, which expressly extends a privilege to a person engaged in, connected with, or employed by "news media."[81] The

80. Sedersten v. Taylor, 2009 WL 4802567 (W.D. Mo. Dec. 9. 2009). Beyond First Amendment protections, other legal privileges may act as a shield to a defamation action. See, e.g., Medcalf v. Walsh, 938 F. Supp. 2d 478 (S.D.N.Y. 2013) (under New York law, a communication from one spouse to another may not be deemed a publication for purposes of defamation, and case law does not reflect an exception for spousal communications made via email, even a corporate network where third parties might be capable of accessing the emails).
81. Too Much Media LLC v. Hale, 20 A.3d 364 (N.J. 2011). See also Obsidian Finance Group, LLC v. Cox, 2011 WL 5999334 (D. Or. Nov. 30, 2011) (self-proclaimed investigative blogger not entitled to protection under Oregon press shield law to protect the identity of her sources because she was not affiliated with any media outlet and the press shield defense is not available in civil defamation actions); but see The Mortgage Specialists, Inc. v. Implode-Explode Heavy Industries Inc., 999 A.2d 184 (N.H. 2010) (website that served an informative function and contributed to the flow of information to the public was entitled to protection under the state's newsgathering privilege and trial court erred in not applying a balancing test to determine whether the plaintiff could overcome the newsgathering privilege in a

state supreme court affirmed the lower court's finding that the defendant's use of a message board was not covered under the Shield Law because she lacked a nexus, relationship or connection to "news media" as defined by the statute. The court stated that online message boards were little more than forums for conversation, akin to unfiltered, unedited letters to the editor, and were not the functional equivalent of the types of news media outlets outlined in the Shield Law. The court commented that while the Shield Law provides broad protection, and that certain online sites could satisfy the law's standards, the court stressed that " We do not believe that the Legislature intended to provide everyone who posts a comment [to an online bulletin board] … an absolute reporter's privilege under the Shield Law."

- **AF Holdings, LLC v. Does 1-1058** – A copyright owner of pornographic films brought an infringement action alleging that 1,058 unknown individuals had used a peer-to-peer file sharing application to download and distribute such copyrighted films.[82] The district court granted the owner's request for subpoenas to the Internet Service Providers (ISPs) that required the ISPs to identify customers associated with certain internet protocol (IP) addresses.[83] In the first paragraph, the opinion noted that the copyright owner was "seek[ing] to manipulate judicial procedures to serve their own improer ends. This case calls upon us to evaluate – and put a stop to – one litigant's attempt to do that."[84] The ISPs argued that the subpoenas designed to reveal the identities of the John Doe defendants were "unduly burdensome" as defined in the Federal Rules of Civil Procedure (FRCP) because venue is improper, personal jurisdiction

---

civil suit where the press is a non-party to a defamation action; In re January 11, 2013, Subpoena by the Grand Jury of Union County New Jersey, No. 13-0001 (N.J. Super. Apr. 12, 2013) (government watchdog blogger that made posts regarding the apparent misuse of government funds is entitled to the press shield privilege because, among other things, she used journalistic methods to uncover newsworthy topics, despite not being a professional journalist that "consistently and exclusively" wrote newsworthy posts).

82. 752 F.3d 990 (D.C. Cir. 2014).
83. See A.F. Holdings, LLC v. Does 1-1058, 286 F.R.D. 39 (D.D.C. 2012), *vacated by*, 752 F.3d 990 (D.C. Cir. 2014). Initially, the ISPs had refused to comply by invoking F.R.C.P. 45(d)(3)(A) which provides that a "district court must quash or modify a subpoena that … subjects a person to undue burden."
84. A.F. Holdings, LLC, 752 F.3d at 992; see also Ingenuity 13 LLC v. John Doe, 2013 WL 1898633 (C.D. Cal. May 6, 2013) (describing the plaintiff's attorney in *A.F. Holdings, LLC* as representing a firm that is a "porno-trolling collective").

over the John Doe defendants is lacking, and the defendants could not be properly joined in one action. In the context of venue and personal jurisdiction, the court ruled against the copyright owner because it concluded that the owner did not have a good faith belief that the discovery it sought would enable it show it had personal jurisdiction over the defendant.[85] Specifically, the copyright owner "could not possibly have a good faith belief that it could successfully sue the majority of the 1,058 John Doe defendants, since it had made no effort to limit these discovery efforts to those defendants who might live or have downloaded the porn at issue while in the District of Columbia. The plaintiff had even requested subpoenas for ISPs that do not even provide service in the District of Columbia, nor had they employed simple geolocation technology to determine whether any of the named defendants could live in D.C. or in close proximity thereto. In a "separate and independent ground for reversal," the defendants could not be joined in this particular action because they were never participating in the same "swarm" of downloading the copyrighted movie, and therefore did not act in "the same transaction, occurrence, or series of transactions or occurrences."

- **Solers Inc. v. Doe** – Before enforcing a subpoena seeking the identity of an anonymous defendant in a defamation action, a court must conduct a preliminary screening to ensure that there is a viable claim that justifies overriding an asserted right to anonymity.[86] In a case of first impression, the D.C. appellate court, after surveying the various standards in other jurisdictions, adopted a test that closely resembled the "summary judgment" standard articulated in *Doe v. Cahill,* 884 A.2d 451 (Del. 2005). When presented with a motion to quash (or to enforce) a subpoena which seeks the identity of an anonymous defendant, courts should (1) ensure that the plaintiff has

85. It based its decision in significant part on the holdings in Oppenheimer Fund, Inc v. Sanders, 437 U.S. 340 (1978). In the case, the court held that representative plaintiffs in a class action could not use discovery tools to secure from the defendant the names of the members of the plaintiff class. It concluded as such because the plaintiffs sought this information for notice of litigation, and not instead for a reason that had any bearing on the issues in the case. See id. at 352; see also id. at 352 n.17 ("[W]hen the purpose of a discovery request is to gather information for use in proceedings other than the pending suit, discovery properly is denied.").

86. Solers Inc. v. Doe, 977 A.2d 941 (D.C. 2009). But see Call of the Wild Movie, LLC v. Smith, 274 F.R.D. 334 (D.D.C. 2011) (First Amendment right of alleged file-sharers to remain anonymous must give way to the plaintiffs' right to use the judicial process to pursue what appear to be meritorious copyright infringement claims).

adequately pleaded the elements of the defamation claim, including proffering evidence creating a genuine issue of material fact on each element of the claim that is within its control;[87] and (2) require that reasonable efforts be made to notify the anonymous defendant that a complaint has been filed and a subpoena has been served and that proceedings be delayed for a reasonable time to allow the defendant an opportunity to respond.

In further proceedings, the appeals court reversed the lower court's order compelling enforcement of the subpoena to identify the anonymous speaker.[88] The court found that plaintiff failed to plead concrete damages suffered as a direct result of the alleged defamation (i.e., lost profits or customers, or even a general impairment of its reputation, beyond the costs expended to investigate the claims that it was using unlicensed software), and otherwise did not overcome John Doe's right to speak anonymously.

With the advent of mass communication, the single-publication rule was created to address the problem that arose from the general rule in defamation or right of publicity cases that each sale or delivery of a copy

87. See e.g., A.Z. v. Doe, 2010 WL 816647 (N.J. Super. Ct. App. Div. Mar. 8, 2010) (subpoena to ISP seeking identity of the sender of an anonymous email quashed because plaintiff failed to establish prima facie case of defamation); Matter of Sandals Resorts Intl. Ltd. v Google Inc., 910 N.Y.S.2d 408 (N.Y. Sup. Ct. 2010) (unpublished) (plaintiff not entitled to discovery of the identity of anonymous emailer because the email in question contained protected assertions of opinion that were not defamatory, particularly since the emailer included links to factual materials that indicated that the message was meant to provoke discussion), *aff'd* Sandals Resorts Intl. Ltd. v Google, Inc., 86 A.D.3d 32 (N.Y. App. Div. 2011) (posted email critical of company practices in Jamaica held nonactionable opinion, an exercise in rhetoric meant to foment an examination of the company; "the anonymity of the e-mail makes it more likely that a reasonable reader would view its assertions with some skepticism and tend to treat its contents as opinion rather than as fact"); LeBlanc v Skinner, 103 A.D.3d 202 (N.Y. App. Div. 2012) (defamation claim based upon blog posting stating that the plaintiff was a "terrorist" was non-actionable hyperbole, since readers in the digital age give less credence to such online statements; however, statement that plaintiff was responsible for placing horse's head in Town Supervisor's pool was defamation per se); but see Deer Consumer Prods., Inc. v. Little, 938 N.Y.S.2d 767 (N.Y. Sup. Ct. 2012) (plaintiff permitted to conduct jurisdictional discovery, to be filed under seal, against anonymous Internet speaker where it has made a prima facie showing of the proposed defamation claim; plaintiff has also demonstrated that the knowledge of the defendant's true identity is materially necessary to advance its defamation claim, as without such identifying information, plaintiff would not be able to properly carry its burden of proving the existence of personal jurisdiction).

88. Solers, Inc. v. Doe, No. 10-1523 (D.C. App. Jan. 12, 2012).

of a newspaper or book containing a defamatory statement constituted a separate publication to a new audience, giving rise to a separate cause of action. Under the single-publication rule, it is the original printing of the defamatory material that starts the statute of limitations clock, not its subsequent circulation and any form of mass communication or aggregate publication – such as the publication of an edition of a book or a periodical, or the broadcast of a single radio or television program – is a single communication and can give rise to only one action for libel. Courts considering the single publication rule in Internet-based defamation cases generally have found it applicable to postings made on websites accessible to the general public.

- **Christoff v. Nestle USA, Inc.** – The California single-publication rule applies to not just libel and defamation but also causes of action for unauthorized commercial use of likeness.[89] The California Supreme Court remanded the case to the trial court for further proceedings to determine when the statute of limitations was triggered for the plaintiff's action and whether the defendant's unauthorized uses of the plaintiff's image (i.e. the printing of product labels and various advertisements for an instant coffee product over a five year period) constituted a "single integrated publication" within the meaning of the single publication rule. The court commented that this was an issue of first impression, namely whether an entire advertising campaign could be considered a single integrated publication, such that the defendant's first use of the plaintiff's image triggered the running of the state of limitations for all subsequent uses in whatever form or media format.
- **Yeager v. Bowlin** – An aviation memorabilia website was a "single integrated publication" and protected against stale privacy claims by the single publication rule.[90] The appeals court affirmed the lower

89. Christoff v. Nestle USA, Inc., 97 Cal. Rptr. 3d 798 (Cal. 2009).
90. Yeager v. Bowlin, 2010 WL 95242 (E.D. Cal. Jan. 6, 2010), *aff'd* 693 F. 3d 1076 (9th Cir. 2012). See also Alberghetti v. Corbis Corp., 713 F. Supp. 2d 971(C.D. Cal. 2010), *aff'd* 476 Fed. Appx. 154 (9th Cir. 2012) (an individual's claims against photo licensing service for posting allegedly infringing images on its website begins to run from the time that the content was first posted online; the court found the plaintiff's claims were time-barred under the single publication rule, rejecting the plaintiff's argument that the online sale of each photo license under a standard license was a separate transaction that restarted the statute of limitations); Roberts v. McAfee Inc., 660 F.3d 1156 (9th Cir. 2011) (defamation claims considered time-barred by single publication rule; court rejects the plaintiff's argument that a press release posted online is republished when the defendant fails

court's grant of summary judgment to the defendant on the plaintiff's right of publicity and trademark claims stemming from the defendant's alleged unauthorized use of the plaintiff's name on its website. The court rejected the plaintiff's argument that the website was republished, and the statute of limitations restarted, each time the defendant added to or revised content on its website, even if the new content did not reference or depict the plaintiff. The court held that a statement on a website is not republished unless the statement itself is substantively altered or added to, or the website is directed to a new audience.

CDA Section 230 Immunity

Section 230 of the Communications Decency Act (CDA) Act protects certain Internet-basedactors from certain kinds of lawsuits. Generally speaking, the statute is designed at once to promote the free exchange of information online and to encourage voluntary monitoring for offensive or obscene material.

There are three essential elements that a party must establish in order to claim Section 230(c)(1) immunity: (1) it is a provider of an interactive computer service; (2) the cause of action treats the defendant as a publisher or speaker of information; and (3) the information at issue is provided by another information content provider. Under the statute, this grant of immunity applies only if the interactive computer service provider is not also "responsible, in whole or in part, for the creation or development of" the offending content. The CDA does not necessarily offer blanket immunity, as the statute does not provide immunity from federal criminal laws, laws "pertaining to intellectual property" and "communications privacy law."[91] The majority of federal courts have interpreted the CDA to grant qualifying service providers broad immunity from civil liability for information originating with a third-party content provider.

Although a fair number of service providers who invoke CDA immunity do so to protect against defamation claims, the language of the statute does not limit its application to such cases. Indeed, many

---

to retract it after receiving notice of its falsity); In re Phila. Newspapers LLC, 2012 WL 3038578 (3d Cir. July 26, 2012) (linking to previously published material is not republication under the single publication rule; "though a link and reference may bring readers' attention to the existence of an article, they do not republish the article").

91. 47 U.S.C. §230(e)(1)-(2), (4).

causes of action might be premised on the publication of what one might call "information content."[92] For example, a provider might get sued for violating anti-discrimination laws, fraud, negligent misrepresentation, and ordinary negligence, and false light. Thus, according to the Ninth Circuit, what matters is not the name of the cause of action—defamation versus negligence versus intentional infliction of emotional distress —what matters is whether the cause of action inherently requires the court to treat the defendant as the "publisher or speaker" of content provided by another.[93] Put simply, courts must ask whether the duty that the plaintiff alleges the defendant violated derives from the defendant's status or conduct as a "publisher or speaker." If it does, CDA Section 230(c)(1) immunity precludes liability.

- **Jones v. Dirty World Entertainment Recordings, LLC –** Section 230(c) of CDA does not grant immunity to a defendant who, by clear and convincing evidence, "developed" defamatory content on his website about the alleged intimate relations of the plaintiff.[94] The court reached the conclusion that the defendant was a "developer" of the content, and therefore not entitled to immunity, on the grounds that: (1) the domain name "dirty.com" functionally encouraged users to submit defamatory content; (2) creating the "Dirty Army," a group putatively designed to respond to anyone who "dared to object to having their character assassinated," evinced an attitude of endorsement towards potentially defamatory content; and (3) by adding his own comments to the defamatory post in question, the defendant effectively ratified the content. Given this evidence, the defendant could not proffer a plausible argument that he was "neutral with respect to the offensiveness of the content" and therefore not "responsible" for it within the meaning of CDA.[95] Rather, the defendant played a

92. Barnes v. Yahoo!, Inc., 570 F.3d 1096 (9th Cir. 2009) (amended opinion).
93. Id. According to the court, publication involves reviewing, editing, and deciding whether to publish or to withdraw from publication third-party content. See also Fair Housing Council of San Fernando Valley v. Roommates.com, 521 F.3d 1157 (9th Cir. 2008) (en banc) ("[A]ny activity that can be boiled down to deciding whether to exclude material that third parties seek to post online is perforce immune under section 230.").
94. 965 F. Supp. 2d 818 (E.D. Ky. 2013).
95. See 47 U.S.C. § 230(f)(3). The court also noted that the salient point for the purposes of determining whether CDA immunity applies is not whether the statement alongside the defamatory post was defamatory in and of itself, but whether the statement effectively adopted and ratified the content contained in the post. In

"significant role in developing the offensive content such that he has no immunity under the CDA."

The decision of the District Court was overturned on appeal by the Sixth Circuit.[96] Under the material contribution test, the court held that the act of encouraging unwelcome content did not render the website operator a developer under the CDA because to conclude otherwise would both defy the desire of Congress to have an "uninhibited, robust, and wide-open internet," and would create "hecklers'" suits aimed at publishers.[97] Likewise, the appellate court held that the decision of the website to ratify or adopt third-party content did not thus render it a creator of developer of such content. A statement *post hoc* to the occurrence of the third-party actionable conduct would "abuse the concept of responsibility" for the existence of the actionable conduct in the first place.[98]

- **Hill v. StubHub, Inc.** – An online ticket reselling website is entitled to CDA immunity for allegedly facilitating the sale of users' tickets that violated the state anti-scalping law because the site did not "sell" the tickets to the plaintiff and was not a developer of relevant third-party content (i.e., the above-market ticket prices posted by individual resellers).[99] The appellate court reversed the lower court and granted summary judgment in favor of the defendant based on CDA immunity. The court concluded that although the record might support a determination that the

---

this case, the statement was found to have ratified the content within the post, thereby excluding the defendant from CDA immunity. See also S.C. v. Dirty World, LLC, No. 11–CV–00392, 2012 WL 3335284 (W.D. Mo. Mar. 12, 2012) (agreeing with the discussion earlier in the footnote).

96. 755 F.3d 398 (6th Cir. 2014).
97. Id. at 413. The material contribution test involves analysis of whether the action of the operator "materially contributed to the alleged unlawfulness of the content" displayed on the website. See Fair Housing Council of San Fernando Valley v. Roommates.com, LLC, 521 F.3d 1157 (9th Cir. 2008).
98. Jones, 755 F.3d at 415; see also Parisi v. Sinclair 774 F. Supp. 2d 310, 316 (D.D.C. 2011) (noting that it would be contrary to the purpose of the CDA to require a court to adopt a fact-based analysis of if and when a defendant adopted particular statements sufficient to revoke immunity). The court in Jones also noted that the name of the website, www.thedirty.com, does not suggest that only illegal or actionable content will be posted.
99. Hill v. Stubhub, Inc., 727 S.E.2d 550 (N.C. Ct. App. 2012). See also Porras v. Stubhub, Inc., 2013 WL 144045 (N.D. Cal. Jan. 11, 2013) (Stubhub not a "ticket seller" under California statute, but a virtual marketplace; defendant not liable for plaintiff's damages for buying bogus ticket).

defendant encouraged the posting of "market-based" prices on its website or was cognizant of the risk that tickets sold on its website would be priced in excess of face value, such evidence did not support a conclusion that the site ensured that unlawful content would be posted. The court rejected the lower court's reasoning that certain customer service features on the site abrogated CDA immunity, finding that none of the features had any impact on the actual price an individual user set for tickets up for sale. Similarly, the court rejected the lower court's reliance on the site's pricing tools that purported encouraged sellers to price tickets unlawfully, concluding that these were "neutral tools" that offered sellers additional information without suggesting, much less requiring, that they should adjust upward the resale prices for tickets. In sum, the court rejected other, often-used arguments against CDA immunity:" [T]he prevailing tendency among decisions construing the relevant statutory language is to hold that the immunity provided by 47 U.S.C. § 230 is (1) not defeated by evidence tending to show that the website had notice of the unlawful posting; (2) not affected by the fact that a website attempts to earn a profit; and (3) not subject to any liability on the basis of "reasonable foreseeability" or "willful blindness" analysis."

- **Milgram v. Orbitz Worldwide, LLC** – Online ticket intermediaries between buyers and ticket sellers that managed the site, processed transactions and collected service fees are protected from state consumer protection violations by CDA Section 230 because the intermediaries are not information content providers of listings created by third-party sellers.[100] The court granted summary judgment to the defendants. The court rejected the plaintiff's argument that the CDA did not apply to the defendants because they were "commercial actors," finding that "the fact that the defendants charge 'service' or 'administrative' fees is irrelevant to the CDA analysis." The court also concluded that the defendants were not information content providers because the ticket sales information that allegedly contained inaccurate or misleading ticket listings originated from third-party sellers and the defendants' involvement in the site design and active maintenance of the sales process, including the ability to remove sellers or alter content, amounted to nothing more than the exercise of a publisher's traditional editorial functions. The court distinguished the

100. Milgram v. Orbitz Worldwide, LLC, No. 142-09 (N.J. Super. Ct. Aug. 26, 2010).

Roommates.com decision, stating that unlike that case, the defendants did not supply the content to which the plaintiffs object (i.e., inaccurate ticket listings), did not ask ticket sellers to provide any information for an unlawful purpose, and did not design the site to violate any federal or state laws: "At best, the defendants here are guilty of 'passive acquiescence in the misconduct of its users,' and even under *Roommates.com*, defendants are entitled to immunity under §230."

- **Blockowicz v. Williams** – A website is not required to comply with an injunction ordering one of its users to remove defamatory online content because the court lacks authority under Federal Rule of Civil Procedure 65 to compel compliance with the injunction since the third-party website was not acting "in concert" with the user who posted the defamatory content.[101] While sympathetic to the plaintiffs' plight, the court refused to compel the website's compliance with the permanent injunction entered against the user. The court rejected the defendant's argument that the website's ongoing promise to publish and never remove statements demonstrates that the website was in active concert or participation with the defendants-users, concluding that the website's tenuous connection to the defendants was insufficient to compel the website's compliance with the court's permanent injunction.
- **Nemet Chevrolet Ltd. v. ConsumerAffairs.com, Inc**. – A consumer-review website that gathered information for use in preparing class action lawsuits is protected by CDA Section 230 immunity from defamation claims for various posts relating to the quality of the plaintiff's business because the plaintiff failed to sufficient plead facts that the website created or developed, in

101. Blockowicz v. Williams, 675 F. Supp. 2d 912 (N.D. Ill. 2009). See also Bobolas v. Does 1-100, 2010 WL 3923880 (D. Ariz. Oct. 1, 2010); Raggi v. Las Vegas Metropolitan Police Dept., 2009 WL 653000 (D. Nev. Mar. 10, 2009) (CDA Section 230 immunizes a union for allegedly defamatory Web postings from its members on a union-operated bulletin board, despite its refusal to remove the postings); Giordano v. Romeo, 76 So. 3d 1100 (Fla. Dist. Ct. App. 2011) (CDA bars court from issuing an injunction against a non-party website operator that refused to comply with a poster's demand to remove defamatory statements previously posted on the website); Karnaby v. Mckenzie, 2012 WL 2149457 (Conn. Super. Ct. May 10, 2012) (unpublished) (injunction forcing removal of post authored by non-identified anonymous web poster denied).

whole or in part, any of the allegedly defamatory postings.[102] The appeals court affirmed the lower court's dismissal of the plaintiff's action. The court rejected the plaintiff's *Roommates.com*-style argument that the defendant was an information content provider based upon the structure and design of the defendant's website and the fact that the site "steered" consumer complaints into specific categories and asked consumers questions about their complaints. The court found that the plaintiff failed to show how a website that is structured to develop information related to class action lawsuits and contacts posters with questions in any way "develops" or "creates" website content or contributed to the alleged "fraudulent nature of the comments at issue." The court also rejected the plaintiff's bare allegations that liability could be found based upon the defendant's revision of consumer complaints, concluding that Section 230 forbids the imposition of publisher liability on a service provider for the exercise of its editorial and self-regulatory functions. Lastly, the court rejected the plaintiff's argument that the defendant fabricated certain posts to attract other consumer complaints since the plaintiff was unable to

102. Nemet Chevrolet Ltd. v. ConsumerAffairs.com, Inc., 591 F.3d 250 (4th Cir. 2009). See also Shiamili v. Real Estate Group of New York, Inc., 952 N.E.2d 1011 (N.Y. 2011) (website operator that chooses and reposts third-party content is protected by CDA immunity from defamation claims; the CDA "does not differentiate between 'neutral' and selective publishers" and "creating an open forum for third-parties to post content — including negative commentary — is at the core of what Section 230 protects"); Parisi v. Sinclair, 774 F. Supp. 2d 310 (D.D.C. 2011) (online booksellers entitled to CDA immunity for posting allegedly defamatory product descriptions about a self-published book sold on the site; however, the court, in dicta, commented that CDA immunity would not extend to physical book and e-book sales just because the underlying transactions took place on the Internet, since liability for sales would not treat the defendants as the "publisher or speaker" of third-party information); Reit v. Yelp!, Inc., 907 N.Y.S.2d 411 (N.Y. Sup. Ct. 2010) (website's selection of the posts it maintains on its site can be considered the selection of material for publication, and accordingly, the website cannot be deemed an information content provider and is immune from liability for defamation under CDA Section 230; "That Yelp allegedly uses "bad" posts in its marketing strategy does not change the nature of the posted data"); Stevo Design Inc. v. SBR Marketing Ltd., 919 F. Supp. 2d 1112 (D. Nev. 2013) (website bulletin board entitled to CDA immunity from state law misappropriation claims because its sporadic editing of posts and its practice of awarding loyalty points for user posts did not make it a "developer" of content; though the defendant encouraged users to visit and interact with the site through its loyalty points system, its encouragement was not specifically directed at illegal publications).

identify the authors of the posts after cross-checking the information with their business records, determining that, without more concrete evidence, the posts in question could simply be "anonymous, falsified by the consumer, or simply missed by [the plaintiff]."

- **Gibson v. Craigslist, Inc.** – A website is entitled to immunity under CDA Section 230 for allegedly failing to police certain merchandise sold on its site (in this case, an advertisement for the sale of a handgun), which thereafter was used in the commission of an assault against the plaintiff.[103] As a preliminary matter, the court concluded that it may consider a CDA Section 230 defense in the context of a motion to dismiss because the elements necessary to make a finding regarding the defendant's immunity were apparent from the face of the complaint and discovery into the defendant's efforts to prevent the sale of illegal goods would not establish a set of facts that would entitle the plaintiff to any relief. In dismissing the plaintiff's complaint, the court concluded that the defendant was entitled to immunity under CDA Section 230 because, among other reasons, the defendant was a provider of an interactive computer service, the handgun advertisement at issue was provided by another information content provider, and the plaintiff's complaint sought to treat the defendant as the publisher or speaker of the advertisement. The court rejected the plaintiff's argument that he does not seek to hold the defendant liable as a speaker or publisher but rather "as a business," finding that such claims regarding monitoring, screening and policing the site were actions quintessentially related to its role as a publisher.
- **Goddard v. Google, Inc. –** A search engine is protected by CDA Section 230 immunity from unfair competition and negligence claims for the display of sponsored advertisements for fraudulent services because the plaintiff failed to allege facts that plausibly would support a conclusion that the search engine created or developed, in whole or in part, any of the fraudulent sponsored

103. Gibson v. Craigslist, Inc., 2009 WL 1704355 (S.D.N.Y. June 15, 2009). See also Dart v. Craigslist, Inc., 665 F. Supp. 2d 961 (N.D. Ill. 2009) (CDA immunity protected a website from claims that the website facilitated prostitution through its "erotic services" category); Inman v. Technicolor USA, Inc., 2011 WL 5829024 (W.D. Pa. Nov. 18, 2011) (alleged sale of harmful vacuum tubes was facilitated by online communications on eBay's website for which eBay may not be held liable under the CDA).

advertisements.[104] The court rejected the plaintiff's *Roommates.com*-style argument that the search engine's keyword suggestion tool encouraged the creation of fraudulent advertisements, finding that a plaintiff may not establish developer liability merely by alleging that a website operator should have known that the availability of certain tools might facilitate the posting of improper content. The court commented that to establish developer liability, substantially greater involvement is required, such as the situation where a website "elicits the allegedly illegal content and makes aggressive use of it in conducting its business."

- **Doe IX v. MySpace, Inc.** – A social network site is entitled to immunity under CDA Section 230(c) for allegedly failing to institute adequate safety measures to prevent sexual predators from communicating with minors on its website.[105] In dismissing

104. Goddard v. Google, Inc., 640 F. Supp. 2d 1193 (N.D. Cal. 2009). See also Getachew v. Google Inc., 491 Fed. Appx. 923 (10th Cir. 2012) (unpublished) (CDA provides immunity for search engine against claims that search results displayed negative items when an individual's name was entered into the search box); Black v. Google Inc., 2010 WL 3222147 (N.D. Cal. Aug. 13, 2010), *aff'd* 457 Fed. Appx. 622 (9th Cir. 2011) (search engine granted CDA immunity for anonymous third-party content; court rejected plaintiff's argument that an interactive computer service could be held liable merely because its programming facilitated the creation of the content at issue); Jurin v. Google, Inc., 695 F. Supp. 2d 1117 (E.D. Cal. 2010) (CDA Section 230 shields search engine from unfair competition and other tort liability for sale of advertising keywords using plaintiff's mark since its Keyword Suggestion Tool merely suggests keywords to competing advertisers so they might refine their content—an editorial function—and as such does not render the search engine an "information content provider"); but see Doctor's Associates, Inc. v. QIP Holders LLC, 2010 WL 669870 (D. Conn. Feb. 19, 2010) (sandwich chain that solicited, reviewed and posted user-submitted videos about its purported superiority to a competitor may not be protected by CDA immunity because there were material issues of fact concerning whether the defendant merely exercised editorial control over the videos or "actively participated in creating or developing the third-party content").

105. Doe IX v. MySpace, Inc., 629 F. Supp. 2d 663 (E.D. Tex. 2009). See also Witkoff v. Topix, Inc., Case No. BC517897 (Cal. Super. Ct. May 14, 2014) (website hosting discussions of drug use which lead to a fatal overdose was immunized under Section 230 since its sole role was letting the discussion occur); Beckman v. Match.com, 2013 WL 2355512 (D. Nev. May 29, 2013) (online dating site immune from negligence claims for allowing plaintiff's attacker to post a profile and otherwise failing to protect the plaintiff from criminal assault); Riggs v. MySpace Inc., 444 Fed. Appx. 986 (9th Cir. 2011) (unpublished) (social network protected by CDA Section 230 against negligence claims from deletion of the plaintiff's account even though the website did not delete other profiles allegedly created by celebrity imposers); Doe v. SexSearch.com, 551 F.3d 412 (6th Cir.

the complaint, the court rejected the plaintiffs' arguments, stating that allegations regarding a failure to implement measures were merely another way of claiming that the defendant was liable for its role as a publisher of online third-party-generated content. The court also rejected the plaintiffs' *Roommates.com*-style argument that the defendant was partially responsible for creating information exchanged between the plaintiff and the sexual predator because it prompted users to enter certain profile information. The court reasoned that *Roommates.com* was distinguishable because the defendant did not require users to enter information as a condition of use, and although the site prompted its users to supplement their profiles with additional information via a list of categories, such conduct was insufficient to hold the defendant out as an information content provider.

However, while CDA immunity applies to a wide host of claims, some recent decisions have uncovered limitations on the scope of CDA Section 230.

- **Doe 14 v. Internet Brands, Inc.** –In this case, a federal appellate court concluded that a social networking website could be held liable under the CDA for negligent failure to warn users.[106] This case involved a website that allowed aspiring models to post information about themselves in the hopes of entering the industry. The plaintiff had posted information about herself on the website and had then been subsequently lured by other users of the site to a fake audition where she was allegedly drugged and raped. She sued the defendant website for negligence based on failure to warn.[107] This claim was dismissed by the district court pursuant

---

2008) (contract and negligent claims against adult online dating site were dismissed because the user failed to allege that the site breached any contractual promise or committed a negligent act, and because the Terms and Conditions expressly disclaimed responsibility for verifying members' ages and any other warranties; court declined to adopt the district court's broad reading of CDA Section 230 immunity and instead decided the case on other state law grounds).

106. 767 F.3d 894 (9th Cir. 2014).

107. Id. California imposes a duty to warn a potential victim of third party harm when a person has a "special relationship to either the person whose conduct needs to be controlled or … to the foreseeable victim of that conduct." See Tarasoff v. Regents of Univ. of California, 51 P.2d 334 (Cal. 1976), superseded by statute, Cal. Civ. Code § 43.92. Doe 14 argued that the defendant had a cognizable special relationship with her and that its failure to warn her of the rape scheme precipitated the incident in which she fell victim to it. These issues were not

to the statutory immunity under the CDA. The Ninth Circuit held that the plaintiff was not attempting to hold the defendant website as a "publisher or speaker" of third party content, nor was she attempting to find the site liable for failure to remove content posted on its website, and therefore the CDA immunity was essentially inapplicable. Rather, since the plaintiff's theory of liability was rooted in the failure of the website to *give a warning to its users* via the site or email of the potential existence of illegal schemes such as the one involving the plaintiff. Ergo, since the CDA immunity only bars liability that treats a website as a publisher of speaker content provided by someone else, such a warning would only involve content provided by the defendant itself, and not any third parties; therefore, this immunity is inapposite to the plaintiff's failure to warn claim.

- **FTC v. Accusearch Inc. –** A website that solicited requests for confidential consumer telephone records protected by law, knew that its paid researchers were obtaining the information through fraud, and charged customers for such information "contributed mightily" to the generation of such unlawful conduct and was not entitled to immunity under CDA Section 230.[108] The appeals court upheld the lower court's order granting the FTC's request for a disgorgement of profits and a permanent injunction barring the defendant from trading in personal information. The court distinguished its prior decision in *Ben Ezra, Weinstein, & Co., Inc. v. Am. Online Inc.*,[109] where the court granted an ISP immunity for republishing inaccurate stock quotes because its conduct was neutral with respect to the erroneous quotes, and commented that if the information solicited by the ISP had been inherently unlawful, as it was in this case, the court's reasoning would necessarily have been different.

- **Barnes v. Yahoo!, Inc. –** Section 230(c)(1) of CDA bars plaintiff's negligent provision of services tort claim based upon a website's failure in its role as publisher to remove offensive content falsely posted about the plaintiff by a third-party.[110] However, the court

---

before the Ninth Circuit at the time, but these background details are important to understand the CDA-related holdings.

108. FTC. v. Accusearch Inc., 570 F.3d 1187 (10th Cir. 2009).
109. 206 F.3d 980 (10th Cir. 2000).
110. Barnes v. Yahoo!, Inc., 570 F.3d 1096 (9th Cir. 2009) (amended opinion). On remand, the district court denied the defendant's further motion to dismiss,

allowed the plaintiff's promissory estoppel contract claim based upon the defendant's alleged broken promise to remove the content and remanded the case for consideration of whether an enforceable contract existed between the parties and whether immunity under CDA Section 230(c)(2), which protects the provider from liability for any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers objectionable, was applicable.

While CDA Section 230(c)(1) protects qualifying providers from liability for third-party content, Section 230(c)(2)(B), on the other hand, covers actions taken to enable or make available to others the technical means to restrict access to objectionable material. This section of the CDA provides protection for "good Samaritan" blocking and screening of offensive material, such that no provider or user of an interactive computer service shall be held liable on account of any action taken to enable or make available the technical means to restrict access to offensive material. Thus, a provider of software or enabling tools that filter, screen, allow, or disallow content that the provider or user considers obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable may not be held liable for any action taken to make available the technical means to restrict access to that material, so long as the qualifying provider enables access by multiple users to a computer server.

- **Holomaxx Technologies v. Microsoft Corp.** — An ISP that blocked, throttled and classified as spam commercial messages from a bulk email marketer was immune from liability under the Good Samaritan screening provisions of CDA Section 230(c)(2).[111]

---

rejecting the defendant's contention that the plaintiff failed to show the necessary detrimental reliance on the defendant's promises to remove the unwanted false dating profiles. Barnes v. Yahoo!, Inc., 2009 WL 4823840 (D. Ore. Dec. 8, 2009). See also Scott P. v. Craigslist, Inc., No. 10-496687 (Cal. Super. Ct. June 2, 2010) (promissory estoppel claim based upon website's alleged broken promise to remove offensive third-party content survives dismissal motion).

111. Holomaxx Technologies v. Microsoft Corp., 2011 WL 865278 (N.D. Cal. Mar. 11, 2011). The plaintiff subsequently filed an amended complaint, which the court dismissed, with prejudice. See Holomaxx v. Microsoft, 783 F. Supp. 2d 1097 (N.D. Cal. 2011) (court reiterated that CDA § 230(c)(2) allows an interactive service provider to establish standards of decency without risking liability for filtering decisions and that the "good faith" immunity is focused upon the provider's subjective intent).

The court dismissed the plaintiff's tort claims, with leave to amend. The court rejected the plaintiff's argument that §230(c)(2) was not intended to immunize the blocking of "routine business e-mails" with unobjectionable content. While no previous court has articulated specific criteria to be used in assessing whether a provider's subjective determination of what is "objectionable" is protected by §230(c)(2), the court stated that the defendant could reasonably conclude that the plaintiff's bulk emails were "harassing" and thus "otherwise objectionable," particularly since the plaintiff acknowledged that it had sent approximately three million e-mails per day through the defendant's servers, and that at least .5% of these were sent to invalid addresses or resulted in user opt-out. The court also found that the plaintiff made only conclusory allegations that the defendant's filtering program was faulty or that it violated industry standards, and could not cite any legal authority for its claim that the defendant had a duty to discuss in detail its reasons for blocking the plaintiff's messages or to provide a remedy for such blocking.

- **Zango Inc. v. Kaspersky Lab Inc.** — An Internet security software distributor is entitled to immunity under CDA Section 230 from a suit claiming that its software interfered with the use of downloadable programs by customers of an online media company when it classified such programs as objectionable adware.[112] The appeals court affirmed the lower court's ruling that the software company was entitled to invoke the protection of § 230(c)(2)(B) for "good Samaritan" blocking and screening of offensive material, which covers actions taken to enable or make available to others the technical means to restrict access to objectionable material. The court held that the software company was a provider of an "interactive computer service" because it was an access software provider that enables computer access by multiple users to a computer server and thus was entitled to immunity for actions taken to make available to others the technical means to screen objectionable material. The court rejected the plaintiff's argument that a computer service is only "interactive" if it enables people to access the Internet or access content found on the Internet, finding

112. Zango Inc. v. Kaspersky Lab Inc., 568 F.3d 1169 (9th Cir. 2009). See also Smith v. Trusted Universal Standards in Electronic Transactions, Inc., 2011 WL 900096 (D.N.J. Mar. 15, 2011) (provider that aided other entities to restrict access to spam email granted immunity under Section 230(c)(2)(A)).

such an interpretation too "narrow " because the statute merely speaks of providing or enabling computer access "by multiple users to a computer server." The court concluded that, consistent with Congressional intent to immunize the providers of blocking software, Section 230(c) immunity applied to Internet content providers as well as to companies that provide filtering tools and "make available software that filters or screens material that the user *or the provider* deems objectionable." The court also refused to read a good faith requirement into Section 230(c)(2)(B), finding that the good Samaritan provision was not written with such a constraint.

SOCIAL NETWORKS AND ONLINE ADVERTISING

In recent years, online social network websites have received a fair amount of media coverage. The attention has not only concerned their rapid growth and enormous popularity, but also, and perhaps more importantly, has focused on the novel privacy issues that have emerged vis-à-vis the sites and their members, as well as what party should be responsible for the posting of offensive or infringing content or for offsite harms that result from social network interactions.

Broadly speaking, an online social network is a structure that allows its members to share personal information and enables personal contacts through a website or other Internet portal. Member pages of "core" social network sites usually contain information and audio and visual content of a personal nature, though such information may vary widely among individual users. Other interactive sites that allow for the viewing and sharing of media or bring together a community of like-minded users often contain social networking features. Often, this data includes the age, gender and personal interests and hobbies of the individual and is shared with others whom the member determines to be "friends."

In some instances, the social network sites themselves have used this data in connection with marketers, albeit in different ways. In turn, this "sharing" has not only stoked the resentment of some social networking members and privacy advocates, but also has drawn the attention of the Federal Trade Commission (FTC), particularly with respect to online behavioral advertising. The FTC defines online behavioral advertising as the tracking of consumers' online activities in order to deliver tailored advertising. The agency notes that in many cases, the information collected is not personally identifiable in the traditional sense – that is, the information does not include the consumer's name, physical address, or similar

identifier – rather, businesses generally use "cookies" to track consumers' activities and associate those activities with a particular computer or device.

In response, the FTC Staff and industry groups, among others, have released best practices guides for this nascent advertising model. Indeed, with the proliferation of social networking sites and the marketing opportunities of behavioral advertising, it is likely that existing privacy issues will continue to emerge as the online public and the sites themselves determine when disclosure of personal information or online activities runs counter to user's expectations, industry principles, and emerging law.

- **FTC Report, "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers"(March 2012)** – In December 2010, the FTC issued a preliminary staff report to address the privacy issues associated with new technologies and business models. The report outlined a proposed framework to guide policymakers and other stakeholders regarding the best practices for consumer privacy. Generally speaking, the proposed framework called on companies to build privacy protections into their business operations, offer simplified choice mechanisms that give consumers more meaningful control, and increase the transparency of their data practices. In its Final Report, the Commission adopted the staff's preliminary framework with certain clarifications and revisions.[113] The FTC recommends that Congress consider baseline privacy legislation and the industry implement the Report's final privacy framework through individual company initiatives and enforceable self-regulation. To the extent the Report's framework goes beyond existing legal requirements, it is not intended

113. See FTC Report, "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers," (March 2012), available at http://www.ftc.gov/os/2012/03/120326privacyreport.pdf. See also In re Compete, Inc., File No. 102 3155 (settlement announced Oct. 22, 2012) (web analytics company agreed to settle FTC charges that it used web-tracking software to collect personal data without disclosing the extent of the information that it was collecting and otherwise failed to honor privacy promises); The U.S. Department of Commerce, Internet Policy Task Force, "Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework," (Dec. 2010) (in its own "green paper," the U.S. Commerce Department stated that diminished trust in data privacy may impede innovative and productive uses of new technologies, such as cloud computing systems and it stressed the need to enlist the expertise of the private technology sector and consult existing best practices to create voluntary codes of conduct that promote informed consent and safeguard consumer information).

to serve as a template for enforcement actions. Echoing the preliminary report, the FTC prompts companies to: (1) adopt a "privacy by design" approach by building privacy protections into their everyday business practices, including providing reasonable security for consumer data, collecting only the data needed for a specific business purpose, retaining data only as long as necessary to fulfill that purpose, safely disposing of data no longer being used, and implementing reasonable procedures to promote data accuracy; (2) offer a simplified choice for businesses and consumers and give consumers the ability to make decisions about their data at a relevant time and context, including through a Do Not Track mechanism; and (3) make information collection and use practices transparent.

The Final Report clarifies at least three important principles from the preliminary report. First, the FTC addressed concerns about undue burden on small business. The Final Report's privacy framework applies to "all commercial entities that collect or use consumer data that can be 'reasonably linked' to a specific consumer, computer, or other device, unless the entity collects only non-sensitive data from fewer than 5,000 consumers per year and does not share the data with third parties." Notably, the framework applies in all commercial contexts, both online and offline. As to the definition of "reasonably linked," the Final Report clarifies that data is not "reasonably linkable" to the extent that a company: (1) takes reasonable measures to ensure that the data is de-identified; (2) publicly commits not to try to re-identify the data; and (3) contractually prohibits downstream recipients from trying to re-identify the data. Second, the FTC revised its approach to how companies should provide consumers with privacy choices. The preliminary report had set forth a list of five categories of "commonly accepted" information collection practices for which companies need not provide consumers with choice (product fulfillment, internal operations, fraud prevention, legal compliance and public purpose, and first-party marketing). Under the Final Report, the Commission set forth a modified approach that focuses on the context of the consumer's interaction with the business. Under this approach, companies would not need to provide choice before collecting and using consumers' data for "practices that are consistent with the context of the transaction, consistent with the company's relationship with the consumer, or as required or specifically authorized by law." Although many of the five "commonly accepted practices" previously identified in the preliminary report would generally meet this standard, there may be

exceptions. For data collection practices requiring choice, the agency stated that companies should offer the choice at a time and in a context in which the consumer is making a decision about his or her data. Moreover, the Report stated that companies should obtain affirmative express consent before (1) using consumer data in a materially different manner than claimed when the data was collected; or (2) collecting sensitive data for certain purposes. Third, the FTC recommends that Congress consider enacting targeted legislation to provide greater transparency for, and control over, the practices of information brokers. The agency also called on Congress to enact legislation addressing data security.

Lastly, the Final Report announced that the agency would focus its future policymaking efforts on five main privacy items: (1) Do Not Track. The FTC summarized current industry efforts on this front, but stressed that it would continue to work with these groups to complete implementation of an easy-to use, persistent, and effective Do Not Track system; (2) Mobile Privacy. The Report calls on mobile service companies to establish standards that address data collection, transfer, use, and disposal, particularly for location data; (3) Data Brokers. To address the issue of transparency and consumer control over data brokers' collection and use of consumer information, the FTC stated that it supports targeted legislation that would provide consumers with access to information about them held by a data broker. The agency also advocated for the creation of a centralized website where data brokers could detail the access rights and other choices regarding consumer data; (4) Large Platform Providers. The Report reemphasizes that large platforms (e.g., ISPs, operating systems, browsers, and social media) that seek to comprehensively track consumers' online activities raise heightened privacy concerns; and (5) Promoting Enforceable Self-Regulatory Codes. The FTC will continue to facilitate the development of industry-specific codes of conduct and will use the FTC Act to take action against companies that engage in unfair or deceptive practices, including the failure to abide by self-regulatory programs they join.

- **FINRA Regulatory Notice 10-6** – In January 2010, the Financial Industry Regulatory Authority ("FINRA"), the independent regulator for securities firms doing business in the United States, issued Regulatory Notice 10-06, a guidance to securities firms and brokers regarding the use of social networking websites for business

purposes.[114] Among its key provisions: (1) *Recordkeeping Responsibilities*: "Every firm that intends to communicate, or permit its associated persons to communicate, through social media sites must first ensure that it can retain records of those communications" as required by law; (2) *Suitability Responsibilities*: Regarding recommendations of specific investment products, the Notice urges firms to adopt specific policies, namely, prohibiting recommendations through social media sites without approval of a registered principal, or in the alternative, maintaining a database of recommendations previously approved by a registered principal that can be accessed by personnel; (3) *Interactive Forums*: Real-time interactive communications from a blog or social network page do not require such approval from a principal prior to posting, yet would require that the firm have in place adequate supervisory procedures to minimize compliance risks, such as lexicon-based or random reviews of such interactive electronic communications; (4) *Social Media Restrictions*: Generally speaking, the Notice requires firms to adopt procedures to ensure that personnel using social media sites are adequately supervised and trained; (5) *Third-Party Content*: FINRA does not deem third-party posts as a firm's public communication subject to approval, content, and filing requirements. However, the Notice states that third-party content might be ascribed to the firm if the firm is "entangled" with the preparation of the content or has "adopted" or implicitly or explicitly endorsed the third-party content.

- **Self-Regulatory Principles for Online Behavioral Advertising (July 2009)** – Leading industry associations developed a set of consumer protection principles for online behavioral advertising, meant to correspond with the FTC Staff Report on the issue.[115] The industry's Self-Regulatory Program is broken down into seven principles, which propose that participating organizations and sites, among other things, clearly disclose data collection and use practices with links and disclosures on the Web page where the

114. FINRA Regulatory Notice 10-6, available at http://www.finra.org/web/groups/industry/@ip/@reg/@notice/documents/notices/p120779.pdf.

115. Am. Ass'n of Advertising Agencies et al., "Self Regulatory Principles for Online Behavioral Advertising" (2009), available at http://www.iab.net/media/file/ven-principles-07-01-09.pdf. See also Article 29 Data Protection Working Party, Opinion 5/2009 on online social networking (June 12, 2009) (independent European advisory body on data protection and privacy issued an opinion informing social network sites on how they can work to comply with the EU data protection law, including the 1995 Data Protection Directive).

advertisement appears; permit consumers to choose whether or not their data will be collected, used, or transferred to another entity for behavioral advertising purposes; prohibit service providers from collecting data for behavioral advertising purposes without affirmative consumer consent; adopt reasonable security practices and limit data retention; obtain consent when making material changes to its data collection practices that results in more data collection; and make special considerations for sensitive data, including not collecting financial account numbers, Social Security numbers, pharmaceutical prescriptions, or medical records for behavioral advertising purposes without consumer consent.

- **Craigslist, Inc. v. 3Taps, Inc.** – A classified ad web service may proceed with contract, trespass, CFAA, and limited copyright claims against several aggregators that scraped or reused Craigslist content without authorization contrary to the site's Terms and in contravention of certain IP address blocks.[116] The court denied the defendants' motion to dismiss, except for copyright claims related to content outside of a two-month window where Craigslist arguably had "exclusive" rights to user content. The court stated that assuming that the CFAA encompasses information generally available to the public such as Craigslist's website, the defendants' continued use of Craigslist content after the clear statements regarding authorization in cease and desist letters and the introduction of technological blocking measures constituted unauthorized access under the statute. Regarding the copyright claims, the court ruled that while Craigslist could assert claims related to content during a two-month window where it had affirmatively acquired an exclusive license for user posts, it dismissed the remaining infringement claims because Craigslist's license to user-created posts submitted outside that time period was pursuant to a license that did not use the phrase "all rights" and did not suggest that the rights granted were "exclusive." Concerning common law trespass, the court found that it was plausible that the defendants' scraping and use of content could have diverted sufficient computing resources to impair Craigslist's website and server functionality, but ultimately, whether the defendants caused actual damage or impairment to Craigslist's systems was a question of fact more appropriate for summary judgment.

116. Craigslist, Inc. v. 3Taps, Inc., 942 F. Supp. 2d 962 (N.D. Cal. 2013).

- **Facebook, Inc. v. Power Ventures, Inc. –** A social network profile aggregating service may be liable for copyright infringement for gaining consent from users to make copies of their social network profile pages and then "scraping" the data from the social network for use on its own site.[117] The court denied the defendant's motion to dismiss, rejecting the defendant's argument that no infringement was possible because the profile user pages were not protected by copyright and the social network site did not hold any rights to user content. The court conceded that the defendant correctly asserted that the social network site did not have a copyright on the user content the defendant sought, but found that if the defendant first had to make a copy of a user's entire profile page in order to collect that user content, and that such action might violate the site's terms of use, citing *Ticketmaster L.L.C. v. RMG Techs, Inc.*[118] The court also refused to dismiss the "indirect" copyright infringement claims, finding that the defendant's inducement of users to exceed their authorized usage and thereby allow the defendant to make copies of their profile pages may support a contributory claim. The court also let stand the social network's DMCA claims for the defendant's automated activities that allegedly circumvented certain anti-scraping technological measures on the site that were designed to protect copyrighted content.

  In further proceedings, the court granted the plaintiff's motion for summary judgment on its CAN-SPAM and CFAA claims.[119] The court rejected the defendant's argument that because Facebook's own servers sent the commercial e-mails at issue, the defendants did not "initiate" the e-mails as a matter of law. The court found that although Facebook servers did automatically send the emails at the instruction of the defendant's software, it was clear that the defendants' actions – in creating a friend referral promotion with

117. Facebook, Inc. v. Power Ventures, Inc., 2009 WL 1299698 (N.D. Cal. May 11, 2009). In further proceedings the court found denied the plaintiff's motion on the pleadings on its state law computer fraud claim, finding that the defendant did not act "without permission" within the meaning of Section 502 of the statute when Facebook account holders utilized the defendant's website to access and manipulate their user content on Facebook, even if such action violated Facebook's Terms of Use. However, the court ruled that to the extent that the plaintiff can prove that in doing so, the defendant Power circumvented Facebook's technical barriers, the defendant may be held liable for violation of Section 502. Facebook, Inc. v. Power Ventures, Inc., 2010 WL 3291750 (N.D. Cal. July 20, 2010).
118. 507 F. Supp. 2d 1096 (C.D. Cal. 2007).
119. Facebook, Inc. v. Power Ventures, Inc., 844 F. Supp. 2d 1025 (N.D. Cal. 2012).

monetary incentives, importing users' friends to the guest list, and authoring the e-mail text – served to "originate" the e-mails as is required by the CAN-SPAM Act. Regarding the CFAA claim, the court found that the defendant circumvented technical barriers to access Facebook site, and thus accessed the site "without authorization" and that the plaintiff established that its losses exceeded the $5000 CFAA threshold by offering evidence of the IT costs of attempting to thwart the unauthorized access into its network.

- **Sambreel Holdings LLC v. Facebook, Inc.** – Antitrust claims against a social network for disabling plaintiff's browser add-on that operated on the Facebook platform and generated online advertising separate from Facebook's own ad impressions were dismissed, with leave to amend, because the plaintiff failed to allege any anti-competitive effects in any forum outside of the Facebook website.[120] The court found that just as Facebook has the right to determine the terms for application developers to use the Facebook platform, "it has a right to dictate the terms on which it will permit its users to use its network and is within its rights to require that its users disable certain products before using its website." The court noted that the complaint did not sufficiently allege that any advertising partners were prohibited from advertising with the defendant outside of Facebook, or that Facebook users were prohibited from viewing the defendant's advertisements or using the defendant's products on other websites.

- **Pietrylo v. Hillstone Restaurant Group –** A jury found that an employer violated federal and state computer privacy laws and was liable for back pay and damages for terminating two employees after gaining unauthorized access to a private MySpace page that was created by the plaintiffs and was critical of the company.[121] The jury concluded that the company violated the federal Stored Communications Act and the New Jersey state computer privacy law when

120. Sambreel Holdings LLC v. Facebook, Inc., 906 F. Supp. 2d 1070 (S.D. Cal. 2012).
121. Pietrylo v. Hillstone Restaurant Group, 2009 WL 3128420 (D. N.J. June 16, 2009) (unpublished). See also Eagle v. Morgan, 2013 WL 943350 (E.D. Pa. Mar. 12, 2013) (employer that took control of and changed passwords to ex-employee's LinkedIn account following termination and used it to promote the new CEO's credentials committed misappropriation of identity and publicity in using the plaintiff's name without consent for commercial or advertising purposes; however, the court awarded $0 damages because the plaintiff failed to establish any damages with reasonable certainty or any concrete business losses caused by the temporary loss of her LinkedIn account).

a manager asked another employee, presumably under the duress of maintaining her employment, for the password to the private MySpace page and then shared its contents with upper management, resulting in the termination of the plaintiffs. The jury also found that the employer was not liable for invasion of privacy.

- **Yath v. Fairview Clinics, M.P.** – The "publicity" element of a state law invasion of privacy claim, which required, in part, that the matter be made public by communicating it to the public at large, was satisfied when private healthcare information was posted on a publicly accessible social network website for 24 hours.[122]
- **Romano v. Steelcase Inc. –** A defendant is entitled to compel production of the plaintiff's social network data (including current and historical, deleted pages and related information) based upon a review of the public portions of the plaintiff's social network pages that allegedly revealed an active lifestyle that conflicted with the plaintiff's injury claims.[123] Rejecting the plaintiff's objections to

122. Yath v. Fairview Clinics, M.P., 767 N.W.2d 34 (Minn. Ct. App. 2009). See also Arenas v. Shed Media, 881 F. Supp. 2d 1181 (C.D. Cal. 2011) (basketball player not likely to succeed on right of publicity claims against reality TV show due to the availability of a "public interest" defense; plaintiff had made aspects of his personal life a matter of public concern based on his series of posts to his Twitter account). But see Lalonde v. Lalonde, 2011 WL 832465 (Ky. App. Feb 25, 2011) (under ordinary circumstances, "[t]here is nothing within the law that requires permission when someone takes a picture and posts it on a Facebook page. There is nothing that requires permission when she [is] "tagged" or identified as a person in those pictures.").

123. Romano v. Steelcase Inc., 907 N.Y.S.2d 650 (N.Y. Sup. Ct. 2010). See also Thompson v. Autoliv ASP, Inc., 2012 WL 2342928 (D. Nev. June 20, 2012) (plaintiff ordered, with certain restrictions, to upload five years of social media materials onto external hard drive for inspection; plaintiff's public Facebook profile provided evidence of the plaintiff's post-accident activities and mental state and were relevant to the claims and defenses in the case). But see McCann v. Harleysville Insurance Co. of New York, 78 A.D.3d 1524 (N.Y. App. Div., 2010) (appellate court affirmed the denial of the defendant's motion to compel a signed authorization for access to the plaintiff's social network account because defendant "failed to establish a factual predicate with respect to the relevancy of the evidence" and essentially sought permission to conduct "a fishing expedition into plaintiff's Facebook account"); Tompkins v. Detroit Metropolitan Airport, 278 F.R.D. 387 (E.D. Mich. 2012) (court declined to allow the defendant to view the plaintiff's entire Facebook account or all posted photographs, finding that public postings and surveillance photographs that showed the plaintiff holding a toy dog and pushing a shopping cart did not belie the plaintiff's claims of injury and were not a sufficient predicate showing that the private Facebook material would be reasonably calculated to lead to the discovery of admissible evidence);

producing her social network data, the court ruled that the information was both material and necessary to the defense of this action and that the plaintiff could not hide relevant information "behind self-regulated privacy settings."

- **The Ass'n of the Bar of the City of New York, Comm. on Professional Ethics, "Obtaining Evidence From Social Networking Websites" –** A lawyer may not attempt to gain access to a social networking website under false pretenses, either directly or through an agent.[124] Rather, a lawyer should rely on discovery procedures sanctioned by the ethical rules and case law to obtain relevant evidence, such as the truthful "friending" of unrepresented parties or by using formal discovery devices such as subpoenas directed to non-parties in possession of information maintained on an individual's social networking page.

Mailhoit v. Home Depot U.S.A., Inc., 285 F.R.D. 566 (C.D. Cal. 2012) (court denies motion to compel social media postings relating to emotional events or reactions as overly vague, but allows discovery into postings between plaintiff and fellow employees that referenced her employment or the ongoing litigation).

124. The Ass'n of the Bar of the City of New York, Comm. on Professional Ethics, "Obtaining Evidence From Social Networking Websites," Formal Opinion 2010-2 (Sept. 2010). See also Oregon State Bar, Formal Opinion No. 2013-189 (Feb. 2013) (lawyer may access publicly available information on a social media site; similarly, a lawyer may send a friend request to access non-public information if the person is not represented by counsel in that matter and no actual representation of disinterest is made by the lawyer; a lawyer may not engage in deception designed to shield the lawyer's identity from the person when making a friend request unless it involves a covert investigation of unlawful activit); NYCLA Committee on Professional Ethics, Formal Opinion No. 743 (May 18, 2011) (a lawyer may search a prospective juror's and sitting juror's social networking profile, provided there is no contact or communication with the prospective or sitting juror and the lawyer does not seek to "friend" jurors, or subscribe to their Twitter accounts, or otherwise contact them; if a lawyer discovers juror misconduct, he or she must promptly bring such misconduct to the attention of the court, under N.Y. Rules of Professional Conduct 3.5(d)); San Diego County Bar Assoc., Legal Ethics Opinion No. 2011-2 (May 24, 2011) (rules of ethics bar an attorney from making an *ex parte* friend request to a represented party because an attorney's communication to a represented party intended to elicit information about the subject matter of the representation is impermissible no matter what words are used in the communication; moreover, an attorney may not send a friend request to an unrepresented witnesses without disclosing the purpose of the request); New York State Bar Ass'n, Comm. on Professional Ethics, Op. 843 (Sept. 10, 2010) (lawyer representing a client in pending litigation may access the public pages of another party's social networking website for the purpose of obtaining possible impeachment material for use in the litigation).

The growth and sophistication of e-commerce sites, online auctions, and search engine sponsored advertisements has increased the possibilities of infringing activities, with trademarks being increasingly more susceptible to impermissible use, copying and linking. As a practical matter, few companies have the resources to stop every trademark violation, especially those corporations that have large portfolios of marks and finite resources for policing the marketplace for potential infringers.

On the one hand, the duty to police trademarks is not so weighty a burden that every infringer must be sued immediately or simultaneously; merely, each holder must reasonably undertake to enforce its rights in its mark.[125] On the other hand, the failure to adequately police one's mark can have unwanted consequences for both the mark itself and the owner, including lost revenue to the company, dilution or genericide of the mark, and lost cache of the brand, to name just a few.

As e-commerce continues to grow, so too does the potential for contributory trademark infringement on popular websites, which, due to the size and sheer number of transactions, can often provide fertile ground for others seeking to engage in the sale and marketing of counterfeit goods. Consequently, mark holders have begun to raise the question of whether these websites are required to assist in eradicating trademark infringement and, if so, to what degree.

- **Tre Milano, LLC v. Amazon.com, Inc. –** A major e-commerce site was not likely liable for contributory trademark infringement when it received notices about suspected counterfeit goods for sale

125. A federal appellate court has held that even a suspended corporation, as an unincorporated association, can sue based on federal common law trademark rights under the Lanham Act. See Southern California Darts Ass'n v. Zaffina, 762 F.3d 921 (9th Cir. 2014). What is actually eligible for trademark protection continues to produce interesting results in all jurisdictions. See, e.g., New York Pizzeria, Inc. v. Syal, –- F. Supp. 3d —, 2014 WL 5343523 (S.D. Tex. 2014) (the flavor of a company's pizza sauces cannot be trademarked because the flavor of the food affects its quality and therefore is a functional element of the product); In re Datapipe, Inc., TTAB No. 85173828 (July 7, 2014) (the mark "your cloud" cannot be registered because it is merely descriptive of the personalized data storage and cloud computing services offered under the mark; based on the meanings of "your" and "cloud," the designation "your cloud" does not "evoke a unique commercial impression," but was rather a situation in which the individual words merely retain their descriptive meanings); see also Herb Reed Enterprises, LLC v. Florida Entertainment Management, Inc., 736 F.3d 1239 (9th Cir. 2014) (a demonstration of irreparable harm is required to grant a preliminary injunction in a trademark infringement suit under the Lanham Act).

on its site without further substantiating evidence confirming "proof of a violation" (e.g., a test buy that confirmed counterfeit goods) and it took no action to remove such infringing listings until it conducted its own investigation.[126] The appellate court affirmed the lower courts' denial of the plaintiff's request for a preliminary injunction barring the defendant from offering to sell the plaintiff's products. Echoing the Second Circuit's landmark *Tiffany* decision[127], the court stated that *Tiffany* and related precedent did not support a conclusion that a listing must be removed—rather than investigated—upon notice that it likely is for a counterfeit product. The court also rejected the argument that the defendant was liable for direct infringement because it was not the seller of the counterfeit goods, but merely facilitated third-party sales by offering product descriptions and offering payment processing and product fulfillment services.

- **Ascentive, LLC v. Opinion Corp. –** A consumer gripe site is not likely liable for direct trademark infringement for its use of the plaintiff's trademarks in subdomains (e.g., <ascentive.pissedconsumer.com>), website metatags, and in the text of its website served by a third-party ad network.[128] The court denied the plaintiffs' motion for a preliminary injunction because plaintiffs were unlikely to succeed on the merits of their Lanham Act and related state claims. The court found that there was no likelihood of confusion based upon the site's use of the plaintiff's trademarks in the PissedConsumer website text and subdomain names because, among other things, the parties were not competitors and the subdomain pages made it clear through their critical language that they were not affiliated with the trademark holders such that no reasonable visitor to the gripe pages would assume the sites were affiliated with the plaintiffs. Interestingly, the court stated that there was no need for the gripe pages to contain a disclaimer as it was evident from the domain name and content that the site was a third-party gripe site for "pissed"

126. Tre Milano, LLC v. Amazon.Com, Inc., 2012 WL 3594380 (Cal. Ct. App. Aug. 22, 2012) (unpublished).
127. Tiffany (NJ) Inc. v. eBay, Inc., 600 F.3d 93 (2d Cir. 2010).
128. Ascentive, LLC v. Opinion Corp., 842 F. Supp. 2d 450 (E.D.N.Y. 2011). See also Dwyer Instruments, Inc. v. Sensocon, Inc., 873 F. Supp. 2d 1015 (N.D. Ind. 2012) (court rejects plaintiff's initial interest confusion claim because plaintiff failed to present evidence to suggest that, even if the defendant intended to increase its Internet traffic through search results for the plaintiff's product, any such purpose was successful achieved or any consumer confusion resulted).

consumers.[129] The court also rejected the plaintiffs' argument that the defendant's use of the plaintiffs' mark in website metatags was likely to cause initial interest confusion, finding that modern search engines make little use of metatags and otherwise declining to rely on Brookfield Communications v. West Coast Entertainment Corp., 174 F.3d 1036 (9th Cir. 1999): "The Court agrees with the criticism that the harm caused by initial interest confusion in the internet context is minimal as 'with one click of the mouse and a few seconds delay, a viewer can return to the search engine's results and resume searching for the original website.'" Regarding the plaintiffs' claims that the defendant employed unscrupulous search engine optimization practices, the court concluded that such transgressions concern the search engines' terms of services, not trademark law. The court also stated that plaintiffs' infringement claims were unlikely to succeed based upon the serving of third-party ads on the site, concluding that plaintiffs failed to assert any authority for the proposition that a website owner can be held liable for direct infringement based on actions by a third-party advertising network on the owner's site. Finally, the court concluded that plaintiffs' related state law claims concerning the negative postings on the defendant's site were barred by CDA Section 230 because PissedConsumer was not a creator or developer of content, despite claims that it encouraged consumers to create negative postings on the site.

- **Louis Vuitton Malletier SA v. Akanoc Solutions, Inc.**, – A web host that ignored multiple takedown notices and knowingly enabled infringing conduct by leasing packages of server space, bandwidth and IP addresses to foreign-based websites that sold knockoff goods is joint and severally liable for a single award of statutory damages for contributory trademark infringement in the amount of $10.5M.[130] The court rejected the defendant's argument that the servers and internet services provided were not the "means of infringement," rather the websites selling the infringing goods were the sole means of infringement. Instead, the appeals court stated that even though they exist in cyberspace, "websites are not ethereal" and would not

129. See also Cintas Corp. v. Unite Here, 601 F. Supp. 2d 571 (S.D.N.Y. 2009) (union that operated critical websites not liable for trademark infringement or unfair competition because there was no likelihood of confusion among users that the websites were affiliated with the company, given the transparent disdain of the text and the prominent disclaimers on the site).

130. Louis Vuitton Malletier SA v. Akanoc Solutions, Inc., 658 F.3d 936 (9th Cir. 2011).

exist without physical roots in servers and internet services and that defendants had direct control over the "master switch" that kept the websites online and available.

- **Tiffany (NJ) Inc. v. eBay, Inc. –** An online auction site that possessed generalized knowledge that counterfeit goods of a well-known brand were sold on its site, but was not willfully blind to infringement and undertook measures to root out and suspend infringing auctions, is not liable for contributory trademark infringement.[131] The appeals court affirmed the judgment in favor of the defendant on the trademark and dilution claims, but remanded for reconsideration the plaintiff's false advertising claim. The court applied the Supreme Court's *Inwood* contributory trademark infringement standard, which requires that a plaintiff prove that the defendant "knows or has reason to know" that it is supplying its product to an infringer and continues to do so. The court rejected the plaintiff's argument that generalized notice that some portion of the plaintiff's goods being sold on the defendant's site were counterfeit required the site to preemptively remedy the problem. The court concluded that: "For contributory trademark infringement liability to lie, a service provider must have more than a general knowledge or reason to know that its service is being used to sell counterfeit goods. Some contemporary knowledge of which particular listings are infringing or will infringe in the future is necessary." Concerning the plaintiff's "willful blindness" argument, the court reasoned that the defendant

131. Tiffany (NJ) Inc. v. eBay, Inc., 600 F.3d 93 (2d Cir. 2010). On remand, the district court dismissed the plaintiff's false advertising claim, finding that there was no extrinsic evidence indicating that the challenged advertisements were misleading or confusing. Tiffany (NJ) Inc. v. eBay, Inc., 2010 WL 3733894 (S.D.N.Y. Sept. 13, 2010). See also Louis Vuitton Malletier v. The Flea Market, Inc., 2009 WL 1625946 (N.D. Cal. June 10, 2009) (a property owner may not be liable for contributory trademark infringement if it only leases property to a separate and distinct entity, which in turn operates a flea market and rents space to a vendor, which in turn infringes trademarks); Sellify Inc. v. Amazon.com, Inc., 2010 WL 4455830 (S.D.N.Y. Nov. 4, 2010) (contributory trademark infringement claims dismissed because there was no evidence that Amazon.com had particularized knowledge of, or direct control over, its affiliate's disparaging, keyword-triggered ads and when Amazon gained knowledge of the ads, it acted promptly to disable the affiliate's account). But see Gucci America, Inc. v. Frontline Processing Corp., 721 F. Supp. 2d 228 (S.D.N.Y. 2010) (famous apparel maker alleged sufficient allegations of contributory trademark infringement against a credit card processing service provider who allegedly induced trademark infringement, and against similar providers that allegedly exerted sufficient control over the infringing transactions and knowingly provided services to a counterfeiter).

did not purposefully avoid learning of counterfeiting on its site, considering the defendant's significant anti-fraud measures and the defendant's prompt removal of infringing listings upon receiving a removal demand under its notice-and-takedown program. The appeals court, however, returned the plaintiff's false advertising claim back to the lower court for reconsideration of whether the defendant was liable for advertising the sale of Tiffany goods on its website when many of those goods were in fact counterfeit. The appeals court noted that the lower court failed to properly evaluate the plaintiff's claim and that it needed to determine whether extrinsic evidence indicated that certain challenged website and keyword advertisements were misleading or confusing to consumers insofar as they implied the genuineness of Tiffany goods on the defendant's auction site.

- **Beltronics USA, Inc. v. Midwest Inventory Distribution, LLC –** The first sale doctrine, which generally limits the right of a producer to control distribution of its trademarked product beyond the first sale of the product, was not available for an eBay merchant that allegedly resold infringing trademarked goods that did not include the associated warranties and services.[132] The court recognized that the unauthorized resale of a "materially different" trademarked product can constitute trademark infringement and concluded that the appropriate test for materiality should not be strictly limited to physical differences, but could include other differences such as warranty protection or service commitments that may well render products non-identical in the relevant Lanham Act sense.

Keyword Advertising and Website Metatags

Internet advertising remains a vital outlet for many businesses looking to reach a wide swath of consumers. To that end, search engine advertisers purchase terms or keywords, which, when entered as a search term, trigger the appearance of the advertiser's online advertisement and link in a prominent place among the page of search results. Under the pay-per-click model, advertisers pay the search engine based on the number of times Internet users click on the advertisement. For example, a company (ABC Company) that sells old LPs can purchase the terms "vintage records" or "vintage LPs" in order to display its advertisement and link whenever a search engine user

132. Beltronics USA, Inc. v. Midwest Inventory Distribution, LLC, 562 F.3d 1067 (10th Cir. 2009).

launches a search based on those search terms. More troublesome to trademark owners, the same company can also cause its ad and link to appear whenever a user searches for the term "ABC Competitor," a competitor of ABC Company in the record sales business. Thus, whenever a searcher interested in purchasing vintage records from ABC Competitor enters a search of the competitor's trademarked name, an advertisement and link would appear on the user's screen, inviting the searcher to ABC Company's store, presumably alongside a link to its competitor.

According to advertisers and the search engine companies, the practice of selling trademarked keywords should be considered a permissible practice that does not cause consumer confusion or is merely a noncommercial use of a trademark that places an advertisement in front of a potential purchaser, which should be no different from other types of competitive/comparative advertising, particularly if the advertiser does not include the trademarked term in its online advertisement. Many trademark owners disagree and consider the use of their marks as keywords to constitute infringement or unfair competition that improperly diverts Internet traffic from their sites and confuses consumers about the source of the products they encounter via pop-up ads, banners and sponsored search results.

- **Network Automation, Inc. v. Advanced Systems Concepts, Inc.** – A software company's purchase of a competitor's trademark as a search engine keyword did not likely cause consumer confusion and constitute trademark infringement under the Lanham Act.[133] The appeals court reversed the district court's grant of a

133. Network Automation, Inc. v. Advanced Systems Concepts, Inc., 638 F.3d 1137 (9th Cir. 2011). See also CollegeSource, Inc. v. AcademyOne, Inc., 2012 WL 5269213 (E.D. Pa. Oct. 25, 2012) (no trademark infringement for keyword advertisements that clearly delineated from search results and do not use the plaintiff's trademark in the advertisement text); College Network Inc. v. Moore Educational Publishers, Inc., 378 Fed. Appx. 403 (5th Cir. 2010) (unpublished) (appeals court affirmed the legal sufficiency of a jury verdict which found that although the plaintiff possessed a valid trademark, the defendant did not infringe it by using it as a search-engine keyword for sponsored advertising and the evidence did not compel a finding of likelihood of confusion); AK Metals LLC v. Norman Industrial Materials Inc., 2013 WL 417323 (S.D. Cal. Jan. 31, 2013) (competitor did not likely commit trademark infringement for purchasing keyword ads based upon the plaintiff's trademark with the header "Ads related to Escondido Metal Supply"; court stressed that the plaintiff failed to meet its burden to show the likelihood of confusion for its preliminary injunction request because the ads in question were clearly separated from the search results and were labeled

preliminary injunction barring Network Automation from using its competitor's trademark as a keyword. The court stated that lower court erred in not flexibly weighing the *Sleekcraft* likelihood of confusion factors to the specific facts of this case and relied on the Internet "troika," which may be helpful in the context of domain names, but is not the correct standard to analyze likelihood of confusion in a keyword case. The court also noted that when a court examines initial interest confusion claims, the trademark owner "must demonstrate likely confusion, not mere diversion." Ultimately, the appeals court stated that the most relevant factors in a keyword case are: (1) the strength of the mark; (2) the evidence of actual confusion; (3) the type of goods and degree of care likely to be exercised by the purchaser (recalling, that the default degree of consumer care is becoming more heightened as online commerce becomes commonplace); and (4) the labeling and appearance of the advertisements and the surrounding context on the screen displaying the results page.

- **Rosetta Stone Ltd. v. Google Inc.** – A reasonable trier of fact could find that a search engine's practice of auctioning a company's trademarks as keywords to third party advertisers creates a likelihood of confusion under the Lanham Act as to the source or origin of the company's goods.[134] The appeals court reversed the grant of summary judgment to the defendant, concluding that there was sufficient evidence in the record to create a question of fact on each of the "disputed" and relevant likelihood of confusion factors—intent, actual confusion, and consumer sophistication— to preclude summary judgment. The court also rejected the lower court's reliance on the functionality doctrine, finding it inapplicable in this case. The court stated the lower court incorrectly focused on whether the plaintiff's Rosetta Stone mark made Google's

---

to minimize confusion); Multi Time Machine, Inc. v. Amazon.com, 926 F. Supp. 2d 1130 (C.D. Cal. 2013) (online retailer that does not carry plaintiff's product but presents a clearly marked list of search results for competing brands when a user enters the plaintiff's trademarked product name into an internal search engine did not commit trademark infringement because users were not confused as to the source of the products displayed in the list of search results); but see Binder v. Disability Group Inc., 772 F. Supp. 2d 1172 (C.D. Cal. 2011) (a law firm's purchase of a competitor's trademark for use in keyword advertising constitutes a use in commerce under the Lanham Act and trademark infringement based upon a finding of likelihood of confusion, with enhanced damages due to the defendant's willful infringement).

134. Rosetta Stone Ltd. v. Google, Inc., 676 F.3d 144 (4th Cir. 2012).

keyword advertising products more useful, neglecting to consider whether the mark was functional as Rosetta Stone used it. The court stated that the plaintiff used its registered mark as a classic source identifier in connection with its language learning products and there was clearly nothing functional about such use. The court also found material issues of fact with regard to the plaintiff's contributory infringement claims regarding the sufficiency of the defendant's response to the plaintiff's written notices alerting Google to the presence of sponsored ads selling counterfeit goods. The appeals court also held that the district court erred when it ruled that the defendant was not liable for dilution simply because there was no evidence that Google used the plaintiff's marks to identify Google's own goods. The court stated that the lower court failed to consider all the required factors – namely, the defendant's good faith use of the plaintiff's mark – when it considered the defendant's nominative fair use defense.

- **Jurin v. Google, Inc.** – A search engine's inclusion of the plaintiff's trademark in its keyword advertising program available to advertisers and competitors does not create a misleading suggestion as to the producer of the good and cannot form a viable false designation of origin claim under the Lanham Act.[135] The court dismissed the plaintiff's remaining trademark and contract claims, with leave to amend. Regarding the false designation of origin claim, the court found that the plaintiff failed to show how the defendant's keyword advertising program misled consumers as to the producer of the plaintiff's trademarked good. The court also dismissed the plaintiff's false advertising claim, concluding that the defendant, a search engine, was not a direct competitor of the plaintiff, a building material manufacturer, even if the defendant "derives its income from third parties who compete for Plaintiff's advertising audience." Lastly, the court dismissed the plaintiff's breach of contract claim based upon its own Google Adwords agreement with the defendant. The court held that the agreement did not require the defendant to investigate the plaintiff's complaint of trademark infringement and remove the trademarked keyword term from its database. According to the court, the defendant was not contractually bound to disable keywords in response to a trademark complaint, but only investigate the use of a trademarked term in ad text only. In a further proceeding, the court granted

135. Jurin v. Google Inc., 2010 WL 3521955 (E.D. Cal. Sept. 8, 2010).

summary judgment in favor of the search engine, finding no evidence of likelihood of confusion or false advertising regarding the search engine's sale of keyword advertising that employs the plaintiff's trademark.[136]

- **Rescuecom Corp. v. Google Inc. –** A search engine's recommendation and sale of trademarked term to advertisers, so as to trigger the appearance of the buyer's advertisements and links, constitutes actionable trademark use under the Lanham Act.[137] The appeals court reversed the district court's dismissal of the plaintiff's trademark infringement action and denied the search engine's motion for summary judgment on the trademark "use" issue. The court rejected the search engine's argument that there was no trademark use based upon evidence that the search engine did not permit purchasers of sponsored links to employ trademarked terms that they did not own in the text or title of their online advertisements. The appeals court also distinguished the search engine's reliance on its precedent in *1-800 Contacts, Inc. v. WhenU.com, Inc.,*[138] where the Second Circuit found no use in commerce when Internet pop-up advertisements were generated based upon users' queries entered in a Web browser and compared to an unpublished directory of terms, which included a markholder's website address/trademark.

  Seemingly narrowing its prior *1-800 Contacts* ruling, the appeals court distinguished the precedent in two ways: (1) in contrast to *1-800 Contacts*, where the defendant made no use whatsoever of the plaintiff's trademark, in the instant case, the court stated that the defendant recommended and sold the plaintiff's mark to its advertisers; (2) in contrast to *1-800 Contacts*, where the defendant did not "use or display," much less sell trademarks as search terms to its advertisers, here the defendant displayed, offered, and

136. Jurin v. Google, Inc., 2012 WL 5011007 (E.D. Cal. Oct. 17, 2012). See also Ison v. Google, No. 10-163032 (Cal. Super. Jan. 22, 2013) (sale of individual's name as keyword is not common law trademark infringement because plaintiff presented no evidence that her name-related marks acquired any secondary meaning); Home Decor Center, Inc. v. Google, Inc., No. 12-05706 (C.D. Cal. May 9, 2013) (search engine's sale of plaintiff's trademark for use in keyword advertising by a competitor not infringement because plaintiff's trademark was generic; related state law claims based upon automated tool that included the trademark in keyword ads was alternatively barred by CDA Section 230).

137. Rescuecom Corp. v. Google Inc., 562 F.3d 123 (2d Cir. 2009).

138. 414 F.3d 400 (2d Cir. 2005).

sold the plaintiff's mark to its customers when selling its paid advertising services. The court made clear that it did not imply in *1-800 Contacts* that an alleged infringer's use of a trademark in an internal software program insulates the alleged infringer from a charge of infringement, no matter how likely the use is to cause confusion in the marketplace. In the end, the court allowed the plaintiff's trademark action to survive a motion to dismiss, but took no position regarding whether the plaintiff could prove likelihood of confusion and ultimately infringement resulting from the search engine's sponsored advertisements.

Domain Name Litigation & Cybersquatting

Many disputes have arisen over the rights to domain names that are identical or similar to existing trademarks. Unrelated companies, competitors, and disgruntled individuals register such domain names, often causing difficulty for the owners of non-famous and famous marks alike. Such registrations may be innocent, or they may be done deliberately in an attempt to gain an unfair commercial advantage over a competitor or obtain financial payment from the holder of the mark (i.e., domain name piracy or "cyberquatting"). Mark holders have sought relief in domain name disputes under federal law, such as the Anti-Cybersquatting Consumer Protection Act (ACPA) and domain name administrative policies adopted specifically to handle domain name disputes (e.g. the ICANN Domain Name Dispute resolution Policy (UDRP)), as well as under federal trademark laws and state unfair competition laws.

- **Petroliam Nasional Berhad v. GoDaddy.com, Inc.** – The holder of the trademark "Petronas," a major oil and gas company in Malaysia, brought a contributory cybersquatting suit under the ACPA against the domain name registrar, GoDaddy.com.[139] The plaintiff had contacted GoDaddy to request that it taken action against a domain name potentially cybserquatting on the Petronas mark. GoDaddy declined on the grounds that it did not host this domain name and the UDRP precluded it from participating in trademark disputes regarding domain name ownership. The Ninth Circuit held that the Act does not create a cause of action for contributory cybersquatting. In citing to the plain text, legislative history and goals of the law, the court affirmed a summary

139. 737 F.3d 546 (9th Cir. 2013).

judgment ruling in favor of a domain name registrar that it was not a contributory cybsersquatter. The court noted that the plain language of the Act did not include provisions for secondary liability, and that if it read that into the Act, it would "expand the range of conduct prohibited by the statute from a bad faith intent to cybersquat to the mere maintenance of a domain name by a registrar, with or without a bad faith intent to profit."[140] It further held that Congress did not incorporate the common law of trademark, including contributory infringement, into the ACPA, as it had into the Lanham Act and as the plaintiff argued in the instant case.[141] Rather, the ACPA did not result from the codification of the common law that included such a cause of action, it had distinct elements from traditional trademark law, and the ACPA itself is narrowly tailored to prohibit primarily the bad faith and abusive regulation of distinctive marks.

- **Toyota Motor Sales, U.S.A. Inc. v. Tabari** – An independent auto broker that specializes in selling Lexus automobiles has certain rights under the nominative fair use doctrine to truthfully use the plaintiff's mark in its domain names (e.g. buy-a-lexus.com), so long as it's unlikely to cause confusion as to sponsorship or endorsement.[142] The circuit court found that the defendant auto

140. According to the *Petroliam Nasional* court, the legislative history of the Act showed that it intended to codify the protection given to registrars by the Ninth Circuit in the case of Lockheed Martin Corp v. Network Solutions, Inc., 194 F.3d 980 (9th Cir. 1999), a case that considered secondary liability for registrars for trademark infringement under the Lanham Act. *See also* S. Rep. 106-140 at 11 ("The bill, as amended, also promotes the continued ease and efficiency users of the current registration system enjoy by codifying current case law limiting the secondary liability of domain name registrars and registries.").

141. Contributory liability has been applied to trademark infringement lawsuits under the Lanham Act, as discussed *supra*. See Central Bank of Denver, N.A. v. First Interstate Bank of Denver, N.A., 511 U.S. 164 (1994) (noting that although there is no general presumption of secondary liability, courts can infer such a cause of action when it appears Congress intended to incorporate it into a statute. As the context and legislative history indicate, the Lanham Act is believed to have codified the existing common law of trademarks. See Moseley v. V Secret Catalogue, Inc., 537 U.S. 418 (2003) ("Traditional trademark infringement law is part of a broader law of unfair competition that has its sources in English common law, and was largely codified in the Trademark Act of 1946 (Lanham Act.)", *superseded by statute on other grounds*, Federal Trademark Dilution Act of 1996, 109 Stat. 985-986, *as recognized in* Levi Strauss & Co v. Abercrombie & Fitch Trading Co., 633 F.3d 1158 (9th Cir. 2011).

142. Toyota Motor Sales, U.S.A. Inc. v. Tabari, 610 F.3d 1171 (9th Cir. 2010). But see DSPT Int'l, Inc. v. Nahum, 624 F.3d 1213 (9th Cir. 2010) (even if a domain

broker used no more of the mark than was necessary to describe its business and that due to a disclaimer, there was no risk of confusion and its use of the plaintiff's mark was fair. The circuit court vacated the district court's injunction ordering relinquishment of the defendant's domain names and remanded the case for further proceedings. The court stated that when a domain name consists *only* of the trademark followed by a suffix like .com (as was not the case here), it will typically suggest sponsorship or endorsement by the trademark holder. However, when a domain name making nominative use of a mark does not actively suggest sponsorship or endorsement, the court reasoned that "the worst that can happen is that some consumers may arrive at the site uncertain as to what they will find" and that "reasonable, prudent and experienced internet consumers are accustomed to such exploration by trial and error." The court concluded by stating: "Outside the special case of trademark.com, or domains that actively claim affiliation with the trademark holder, consumers don't form any firm expectations about the sponsorship of a website until they've seen the landing page—if then. This is sensible agnosticism, not consumer confusion." The court also clarified the burden of proof when nominative fair use is raised, holding that a defendant seeking to assert nominative fair use as a defense need only show that it used the mark to refer to the trademarked good, and then the burden reverts to the mark holder to show a likelihood of confusion; in short, the nominative fair use" analysis replaces the traditional multipart likelihood of confusion test as the proper measure for determining consumer confusion whenever defendant asserts to have referred to the trademarked good itself.

- **Solid Host NL v. NameCheap Inc.** – A registrar that provided an anonymous domain name registration proxy service may be liable for cybersquatting when it refused to reveal the identity of a hacker who allegedly obtain the plaintiff's domain name without authorization after receiving a formal demand with accompanying

---

name was put up innocently and used properly for years, a person is liable for cybersquatting if he subsequently uses the domain name with a bad faith intent to profit from the protected mark by holding the domain name for ransom; appeals court affirmed a jury verdict finding ex-employee who used a domain name as leverage to get his ex-employer to pay him the disputed commissions liable for cybersquatting).

facts concerning the domain name theft.[143] At this early stage of litigation, the court refused to dismiss the plaintiff's contributory cybersquatting claim. The court ultimately ruled that the plaintiff's complaint, which alleged that the defendant registrar had the ability to monitor and control the instrumentality used by the hacker to engage in cybersquatting, satisfied the direct control and monitoring requirement necessary to plead a contributory liability claim. The court commented that it was a question of first impression whether the statutory protection afforded registrars in §1114(2)(D) of the ACPA applied to registrars who provide services other than processing applications for domain name registration, simply by virtue of their status as accredited registrars. The court further stated that nothing in prior decisions suggested that a registrar is immune under the ACPA when it acts other than as a registrar; indeed, to the extent that the defendant registrar was the registrant of the domain name and "used" the name, the ACPA would support the imposition of liability on it, not a grant of immunity to it.

- **Balsam v. Tucows Inc.** – The ICANN Registrar Accreditation Agreement (RAA), which in part, contains certain disclosure requirements for domain name registrars offering private registration services when domain name holders have been shown to have committed actionable harm, is not intended to benefit third-parties seeking to uncover the identity of a domain name holder.[144] The court dismissed the plaintiff's complaint seeking to compel the registrar to satisfy a default judgment against an unnamed domain name holder that used the registrar's proxy service and

143. Solid Host NL v. NameCheap Inc., 652 F. Supp. 2d 1092 (C.D. Cal. 2009). See also Transamerica Corp. v. Moniker Online Services LLC, 672 F. Supp. 2d 1353 (S.D. Fla. 2009) (trademark holder may proceed with ACPA claim against registrar based upon allegations that the registrar provided services to domain name registrants for infringing domain names and was part of a scheme to profit from their misuse; the court noted that while a registrar is generally not liable under the ACPA, such immunity applied only when the registrar was acting as a registrar); Louis Vuitton Malletier S.A. v. 100Wholesale.com, No. 12-21778 (S.D. Fla. Amended Preliminary Injunction Nov. 30, 2012) (mark holder brought suit against a host of cybersquatters, not under the UDRP or under the in rem provisions of the ACPA, but as an action based upon counterfeiting actions of the domain name registrants in infringing the plaintiff's mark; injunction bars further infringement and transfers domain name registration to the plaintiff's attorney and allows plaintiff to obtain identities of registrants from proxy services).

144. Balsam v. Tucows Inc., 2009 WL 3463923 (N.D. Cal. Oct. 23, 2009), *aff'd* 627 F.3d 1158 (9th Cir. 2010).

held that the "No Third Party Beneficiaries" clause of the RAA was controlling and that plaintiff's contract and related claims stemming from a third-party beneficiary theory failed as a matter of law. The court found that while it was possible for parties to intend to benefit third parties despite contractual language disclaiming third party beneficiaries, the parties to the ICANN RAA evidenced no such intent. The court also rejected the plaintiff's argument that a specific clause trumped the RAA's "general" disclaimer of third party beneficiaries because the section did not bind the parties to the Tucows-ICANN agreement. The court stated that the ICANN RAA, specifically section 3.7.7, required the defendant registrar include such a provision in future contracts between it and parties to whom it registered domain names, but that the provision itself did not by itself bind ICANN or the defendant. As such, the court ruled that since the RAA section 3.7.7 was not truly a clause of the defendant-registrar's agreement with ICANN and it did not "trump" the contract's general disclaimer of third party beneficiaries.

- **Office Depot Inc. v. Zuccarini** – Under California law, domain names domain names are intangible property subject to a writ of execution to satisfy a judgment and are located where the domain name registry is located for the purpose of asserting *quasi in rem* jurisdiction.[145] The Ninth Circuit affirmed the lower court ruling, which permitted the appointment of a receiver to assist in executing a judgment against the defendant through the sale of many of his domain names. Looking to the procedures for obtaining *in rem* jurisdiction under the ACPA, the court found that because domain name registry had its headquarters within the district, the district court had *quasi in rem* jurisdiction over the defendant's domain names registered with that domain name registry. Although the question was not directly before it, the court, in dicta, suggested that it saw no reason why domain names would not also be located where the relevant domain name registrar was located.
- **Southern Grouts & Mortars, Inc. v. 3M Co.** – A party that kept control of a domain name it had registered prior to the mark holder's initial use of the mark in question for the purpose of preventing others from registering the domain name, as opposed to seeking to extort payment from the mark holder, has not

145. Office Depot Inc. v. Zuccarini, 596 F.3d 696 (9th Cir. 2010).

demonstrated a "bad faith intent to profit" required to prove a violation of the ACPA.[146]

PRIVACY RIGHTS AND DATA SECURITY

There is no comprehensive set of privacy rights or legislation in the United States addressing the collection, storage, transmission or use of personal information on the Internet or in other business environments. Instead, privacy has generally been protected by common law and by federal and state legislation enacted as new technologies develop, to target specific privacy-related issues.

For example, the Electronic Communications Privacy Act (ECPA) is the federal statute that updated wiretapping laws to include protection for electronic communications, such as emails. The Act further proscribes the intentional use of the contents of any wire, oral, or electronic communication, that was obtained through the interception of a communication and allows for both criminal penalties and civil causes of action for violations of its provisions. Specifically, the ECPA protects "point-to-point" electronic communications, or communications as they travel through cyberspace. The ECPA contains two sections: Title 1 amended the Wiretap Act, and Title II created the Stored Communications Act. Consequently, the ECPA established a two-tier system, creating separate categories of violations predicated upon whether the electronic communications are accessed while "in transit" or while "in storage."

Although many privacy laws address the government's use of personal information, many others address the use of personal information by private entities, whether it be financial, medical, or sensitive consumer information, commercial messages sent via email, facsimile or SMS, or electronic data intercepted during transmission or improperly accessed from data storage. Moreover, federal and state data security laws that impact electronic privacy concerns have recently been enacted to stem

146. Southern Grouts & Mortars, Inc. v. 3M Co., 575 F.3d 1325 (11th Cir. 2009); see also Foreword Magazine, Inc. v. Overdrive, Inc., 2011 WL 5169384 (W.D. Mich. Oct. 31, 2011) (evidence of solicitation for payment of alleging infringing domain name admissible when claim was not yet disputed, but discussions over payment between defendant's attorney and plaintiff after cease and desist letter was sent were protected by Fed. R. Evid. 408); but see Newport News Holding Co v. Virtual City Vision, Inc., 650 F.3d 423 (4th Cir. 2011) (when defendant abandoned its purpose of providing a city-based information website that was previously found legitimate in a UDRP proceeding and reformatted the site to focus on women's fashions in competition with the plaintiff-mark holder supported a finding of bad faith under the ACPA).

the scourge of malicious software and identity theft, and at least 46 states have passed some form of a data security breach notification law requiring notice in the event of a qualifying data breach of sensitive consumer information.

Advances in Internet technology have also allowed website operators and advertisers to collect, compile and distribute personal information about users' Internet browsing activities, both with and without the user's consent. Such practices will almost always implicate privacy concerns.

- **Riley v. California** – In 2014, the Supreme Court held that the qualities of digital data, particularly data held on a cell phone, make them distinguishable from physical items for the purposes of the Fourth Amendment's privacy protections.[147] In one of the two cases consolidated on appeal, the petitioner was stopped for a traffic violation, upon which an officer searched his cell phone without a warrant. The officer accessed information on the phone and noticed the repeated use of a term associated with a street gang. At the police station two hours later, a detective specializing in gangs examined the phone and unearthed photos and video that tied the petitioner with a shooting that had occurred a few weeks earlier. Based on this information, the petitioner was charged, with a request for an enhanced sentence based on his purported gang affiliation, in connection with the shooting. The court noted that neither of the rationales for a search incident to lawful arrest: (1) harm to officers and (2) destruction of evidence, are applicable when the search is of digital data.[148] Digital data cannot be used as a weapon nor can it serve as evidence that can be destroyed by the arrestee.[149]

147. 134 S. Ct. 2473, 2488 (2014). In rejecting the government's argument that a search of all data stored on a cell phone is "materially indistinguishable" from searches of physical items, the majority opinion responded that this is like "saying a ride on a horseback is materially indistinguishable from a flight to the moon. Both are ways of getting from point A to point B, but little else justifies lumping them together." Id.
148. Riley, 134 S. Ct. at 2484-85. In Chimel v. California, 395 U.S. 752 (1969), the court formulated the warrantless "search incident to arrest doctrine" in which a police officer is permitted to search the person arrested in "order to remove any weapons that the latter might seek to use in order to resist arrest or effect his escape." Id. at 762-63. This doctrine also considers it "entirely reasonable" for the officer to "search for and seize any evidence on the arrestee's person in order to prevent its concealment or destruction." Id. This search is limited to the area within the immediate control of the arrestee. Id.
149. Riley v. California, 134 S. Ct. 2473, 2486 (2014) (citing Chimel, 395 U.S. at 763-64). The petitioner did concede that officers without a warrant could have

Moreover, cell phones and the digital data contained therein, allow for a more intrusive search, and therefore raises heightened privacy concerns. The term cell phone is "itself a misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone." Moreover, because of the "immense storage capacity" of modern cellphones, the intrusion on privacy is not physically limited in the same way. This storage capacity allows a person in possession of the phone to potentially reconstruct a person's private life, or view apps that can serve as proxies for the interests or foibles of a person.

- **Joffe v. Google, Inc.** – Plaintiffs filed putative class actions alleging that Google violated the ECPA and numerous state laws by collecting data from unencrypted wireless local area (Wi-Fi) networks. A primary exception to the ECPA provides that it is permissible to intercept an "electronic communication made through an electronic communication system" is the system is configured so that it is "readily accessible to the general public."[150] In 2013, the Ninth Circuit issued an amended opinion which held that payload data transmitted over unencrypted Wi-Fi networks did not constitute "electronic communications" within the meaning of the ECPA, therefore the acquisition of the payload data did not fall under the exception for data "readily available to the general public."[151] Specifically, the Wi-Fi payload data did not constitute a "radio communication" under 18 U.S.C. § 2510(16). Therefore, since "radio communication" is considered an "electronic communication," if the payload data was not a "radio communication," it could thus be considered for the exception for types of "electronic communications" that are allowed to utilize this exception.

---

seized and secured his cell phone to prevent destruction of evidence. Id. at 2486 (citing Illinois v. McArthur, 531 U.S. 326, 331-33 (2001)). However, this concern evaporates once the officers secure the phone, as the arrestee is no longer able to delete incriminating data. The respondent argued that this information could nonetheless be deleted either by remote wiping and data encryption. Id. The court found these rationales unavailing insofar as they referred to the actions of third parties that have occurred in a small number of isolated instances, at best. Id. at 2486 (citing a number of briefs in support of petitioners).

150. 18 U.S.C. § 2511(2)(g)(i).

151. 746 F.3d 920 (9th Cir. 2013), *cert. denied*, 134 S. Ct. 2877 (2014). This iteration of the Ninth Circuit opinion came after the grant of a petition to rehear the original Ninth Circuit opinion. See Joffe v. Google, Inc., 729 F.3d 1262 (9th Cir. 2013).

- **In re Google Inc. Privacy Policy Litig. –** A search engine's creation of a single, universal privacy policy that eliminated separate privacy policies and allowed it to cross- reference and use consumers' personal information across its multiple online products did not result in a cognizable injury under federal or state privacy statutes. The court dismissed the plaintiff's complaint for lack of standing, with leave to amend.[152] The court found that plaintiffs failed to identify a concrete harm from the alleged combination of their personal information across Google's products sufficient to create an injury, and noted that "nothing in the precedent of the Ninth Circuit or other appellate courts confers standing on a party that has brought statutory or common law claims based on nothing more than the unauthorized disclosure of personal information, let alone an unauthorized disclosure by a defendant to itself."
- **Pirozzi v. Apple Inc. –** A user who brought a putative class action against a mobile device manufacturer for failing to prevent third-party apps distributed through its online App Store from uploading user information from their mobile devices without permission lacks Article III standing because the complaint failed to allege specifics on purchased Apple devices, which company statements were misleading, or otherwise offer evidence that an app developer misappropriated her personal information.[153] The court dismissed the complaint, with leave to amend. The court found that the plaintiff's first claim – that she overpaid for her Apple device or was induced to purchase a device – was lacking because plaintiff failed to allege specifically which statements she found material to her decision to purchase an Apple device or app. On the plaintiff's second claim - misappropriation of her personal information – the court stated that the plaintiff failed to plead that a third-party app developer actually misappropriated her personal information, only that her personal information was at a greater risk of being misappropriated, and concluded that such hypothetical allegations of future harm were insufficient to confer standing. Interestingly, the court refused to dismiss the action based upon CDA Section 230 immunity, finding that, at this early stage, plaintiff's claims that Apple somehow misled Plaintiff as to the "nature and integrity of Apple's products" and induced plaintiff to purchase an Apple device would not seek

152. In re Google, Inc. Privacy Policy Litigation, 2012 WL 6738343 (N.D. Cal. Dec. 28, 2012).
153. Pirozzi v. Apple Inc., 913 F. Supp. 2d 840 (N.D. Cal. 2012).

to hold Apple liable making third-party apps available on its website, but treated Apple as the "information content provider" for the statements at issue.

- **Patco Constr. Co. v. People's United Bank –** A bank's security procedures provided to a commercial account holder that was the victim of fraudulent wire transfers were not commercially reasonable under UCC Article 4A.[154] The appeals court reversed the lower court's grant of summary judgment to the bank and remanded the case. The court concluded that the bank, whose security system prompted users logging in to answer challenge questions on any transaction over $1, increased the risk that such answers would be captured by keyloggers or other malware. Moreover, the court concluded that the bank's failure to monitor and immediately notify customers of abnormal transactions that had been flagged by its security software was not commercially reasonable. The court stated that such collective failures taken as a whole rendered the bank's security system commercially unreasonable under the UCC. The appeals court also reinstated some of the plaintiff's common law claims, finding that while Article 4A displaced the plaintiff's negligence claim, the plaintiff's breach of contract and breach of fiduciary duty were not preempted by Article 4A because such claims were not inherently inconsistent or in conflict with the plaintiff's overarching Article 4A claim. However, despite ruling that the bank's security procedures were not commercially reasonable, the appeals court affirmed the denial of the plaintiff's summary judgment claim. The court noted several disputed issues of fact surrounding the question of whether the plaintiff had satisfied its obligations and responsibilities under Article 4A, or at least to the question of damages.
- **Keller v. Electronic Arts, Inc.** – A former college athlete may proceed with right of publicity claims against a video game maker

154. Patco Constr. Co., Inc. v. People's United Bank, 684 F. 3d 197 (1st Cir. 2012) see also Experi-Metal, Inc. v. Comerica Bank, 2011 WL 2433383 (E.D. Mich. June 13, 2011) (court finds a genuine issue of material fact as to whether the defendant bank accepted in "good faith" fraudulent wire transfers initiated by unknown phishers in the plaintiff's name); Chavez v. Mercantil Commercebank N.A, 701 F.3d 896 (11th Cir. 2012) (bank could not rely on Article 4A safe harbor for account holder's loss from fraudulent in-person transaction because the agreed-upon security procedure did not specify what the bank would do to verify a payment order, and did not even require a signature comparison, so it was not in fact a "security procedure" under the UCC).

that designed a game with virtual football players to resemble real-life college football athletes because the game maker's use of the player's image was not sufficiently transformative such that the First Amendment would bar his California right of publicity claims as a matter of law.[155] The court stated that the game maker's use of the player's image was not transformative because the game presented virtual players that were nearly identical to their real-life counterparts (i.e. sharing the same jersey numbers, similar physical characteristics and background information); depicted the plaintiff in the same setting he was known for, namely, a collegiate football field; and allowed users to download actual team rosters and players' names into the game. The court distinguished the Eighth Circuit's holding in *C.B.C. Distribution and Marketing v. Major League Baseball Advanced Media*, 505 F.3d 818, 820-21 (8th Cir. 2007), which involved a company's use of player's names and statistics for "fantasy sports" games, concluding that the defendant's game "does not merely report or publish Plaintiff's statistics and abilities. On the contrary, [the defendant] enables the consumer to assume the identity of various student athletes and compete in simulated college football matches."

- **Hayes v. SpectorSoft Corp.** – An individual who was the victim of his ex-spouse's installation of keylogging software on his computer cannot bring federal communications privacy or state law negligence claims against the software maker for his emotional distress

155. Keller v. Electronic Arts, Inc., 2010 WL 530108 (N.D. Cal. Feb. 8, 2010); but see The University of Alabama Board of Trustees v. New Life Art, Inc., 683 F.3d 1266 (11th Cir. 2012) (artist's First Amendment interests clearly outweigh whatever consumer confusion that might exist concerning his paintings depicting University of Alabama football games; Lanham Act claims over the sale of paintings, prints and calendars that include the University's football crimson and white uniforms are dismissed); Hart v. Electronic Arts, Inc., 717 F.3d 141 (3d Cir. 2013) (use of a former college football player's image in a NCAA football videogame was not transformative and the game maker was not entitled to summary judgment on the plaintiff's right of publicity claim; the various digitized sights and sounds in the video game's digital recreation of college football and the users' ability to alter the digital avatar did not alter or transform the use of the plaintiff's identity in a significant way); Habush v. Cannon, 2013 WI App 34, 828 N.W.2d 876 (attorneys right of publicity claims against a competing law firm that purchased their last names as keywords was dismissed because the invisible use of purchased keywords for competitive advertising was not a "use" of a name for advertising purposes within the meaning of the Wisconsin privacy statute).

and humiliation. The court dismissed the plaintiff's complaint.[156] The court found that the plaintiff's federal communications privacy claim failed because plaintiff failed to rebut evidence of the software maker's lack of intent to divulge the plaintiff's private communications and the software maker's right to expect that its software should be used in accordance with the accompanying licensing agreement. In addition, the court dismissed the plaintiff's product liability claim, finding it noticeably lacking in any suggestion of the kind of injury required by Tennessee law, namely, personal injury, death, or property damage. The court also deemed the plaintiff's negligence claim deficient, concluding that there was no authority suggesting that a manufacturer of monitoring software owed a duty to avoid emotional injury to the victim of the misuse of that software in violation of the software's licensing agreement.

- **Zheng v. Yahoo! Inc.** – There is no language in the Electronic Communication Privacy Act (ECPA) itself, nor to any statement in the legislative history that indicates Congress intended that the statute apply to activities occurring outside the United States.[157] The court dismissed the plaintiff's federal electronic privacy-related claims stemming from an alleged disclosure of user information to Chinese authorities. The court also rejected the plaintiffs' argument

156. Hayes v. SpectorSoft Corp., 2009 WL 3713284 (E.D. Tenn. Nov. 3, 2009); see also Kirch v. Embarq Management, 702 F.3d 1245 (10th Cir. 2012) (ISP that authorized NebuAd, an online advertising company, to conduct technology tests on internet traffic for directing online advertising is not liable under ECPA because the statute does not allow for civil aiding and abetting liability and regardless, the ISP's access was not an "interception" since it was in the ordinary course of its core business as an ISP transmitting data over its equipment); Luis v. Zang, 2013 WL 811816 (S.D. Ohio Mar. 5, 2013) (court dismissed plaintiff's claims against software maker for ECPA violations where an individual purchased and installed the keylogging software that allowed unauthorized access to the plaintiff's communications; the language of the statute did not contemplate imposing civil liability on software manufacturers and distributers for the activities of third parties in intercepting electronic communication); but see Klumb v. Goan, 884 F. Supp. 2d 644 (E.D. Tenn. 2012) ("interception" occurs when spyware automatically routes a copy of an email, which is sent through the internet, back through the internet to a third party's email address when the intended recipient opens the email for the first time).

157. Zheng v. Yahoo! Inc., 2009 WL 4430297 (N.D. Cal. Dec. 2, 2009). But see Suzlon Energy Ltd. v. Sridhar, 2011 WL 4537843 (9th Cir. Oct. 3, 2011) (the protections of the ECPA extend to the contents of communications of foreign citizens; however, "the Court does not address here whether the ECPA applies to documents stored or acts occurring outside of the United States).

that because the defendant email provider had servers located around the globe, email communications may have traveled through the defendant's networks located in the United States. The court stated that because the alleged interceptions and disclosures occurred "locally" within China, the ECPA did not apply, even if the communications, prior to their interception and disclosure, traveled electronically through a network located in the United States.

- **Quon v. Arch Wireless Operating Co., Inc.** – Under the Stored Communications Act (SCA), a text message service is prohibited from disclosing contents of text messages, absent the consent of the addressee or intended recipient of such communications.[158] The appeals court reversed the lower court's ruling that the text message service permissibly released transcripts of the plaintiff-police officer's text messages sent and received from his work-issued pager for the purpose of an audit by his employer. The court also ruled that the government employer had violated the employer's reasonable expectation of privacy under the Fourth Amendment. The court found that, under the SCA, the text message service was an "electronic communication service" (i.e., any service which provides to users thereof the ability to send or receive wire or electronic communications). Accordingly, the text message service was prohibited from releasing the contents of a communication without the lawful consent of the addressee or intended recipient.

  In further proceedings, the Supreme Court granted certiorari on the sole issue of ruling on the Ninth Circuit's holding that the city employer violated the Fourth Amendment.[159] The Court was reticent to fashion a general principle about electronic privacy around text messages sent or received by government employees and decided the case on narrower grounds. The court stated that even assuming the city employee had a reasonable expectation of privacy in his text messages, the city did not necessarily violate the Fourth Amendment by obtaining and reviewing the transcripts of the messages because (1) there were reasonable grounds for suspecting that the search was necessary for a non-investigatory work-related purpose; (2) the review of the transcripts was an efficient and expedient way to determine whether the employee's excess usage was due to personal use; and (3) even if the SCA forbade the cellular phone carrier from

158. Quon v. Arch Wireless Operating Co., Inc., 529 F. 3d 892 (9th Cir. 2008).
159. City of Ontario, California v. Quon, 130 S.Ct. 2619 (2010).

turning over the transcripts, it did not follow that the city's actions were unreasonable under the Fourth Amendment.

- **Boring v. Google, Inc. –** Residents' state privacy claims against a search engine that offered online "street view" mapping images from their private driveway, including images of the outside of the plaintiffs' residence, are not cognizable because such conduct would not be highly offensive to a person of ordinary sensibilities.[160] The appeals court affirmed the dismissal of privacy and negligence claims against the search engine, but reversed the lower court's dismissal of the plaintiffs' trespass claim. The court allowed the trespass claim to go forward because the plaintiffs alleged that the defendant entered their property without permission, which, if proven, would constitute a trespass. The court commented that there is no requirement under Pennsylvania law that damages be pled, either nominal or consequential, in trespass cases, even though "it may well be that, when it comes to proving damages from the alleged trespass, the [plaintiffs] are left to collect one dollar and whatever sense of vindication that may bring."

Privacy-Related Enforcement Actions

The Federal Trade Commission (FTC) has taken an active role with respect to protecting privacy rights in connection with the collection and use of personal information for commercial purposes. Most notably, the FTC has undertaken enforcement actions against entities that sold information to third parties for commercial purposes contrary to a website privacy policy, failed to keep consumer information secure, installed malicious spyware or adware onto unknowing consumers' computers, or violated the federal do-not-call list with an unlawful telemarketing campaign. In addition, federal civil rights laws and the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, together protect individuals' rights of nondiscrimination and health information privacy, with enforcement falling upon the Department of Health and Human Services' Office of Civil Rights.

- **FTC v. Wyndham Worldwide Corp.** – In recent years, the FTC has begun to take action against companies that are perceived to have insufficient or unreasonable data security policies and/or practices. For example, in 2014 the Federal Trade Commission

160. Boring v. Google Inc., 2010 WL 318281 (3rd Cir. Jan. 28, 2010).

(FTC) brought an action against a hotel conglomerate for violations of the FTC Act (the Act) alleging that the conglomerate failed to maintain reasonable and appropriate data security procedures to protect consumers' PII.[161] These allegedly deficient data security procedures had earlier led to three separate breaches of the company's computers systems, breaches which led to a theft of consumers' payment card account numbers, among other PII.[162] The court initially noted that the defendants essentially asked for an "exception" for data security protocols from the FTC's authority under the unfairness prong of the Act. Moreover, the defendant could not show that the FTC authority over data security would "plainly contradict congressional policy."[163] The court a;sp held that, even though the FTC had not produced a set of formal rules and regulations prior to the filing of this claim, the defendant could not claim a lack of fair notice of what conduct that is either forbidden or required as a result. This claim failed because the FTC was not *required* to issue rules and regulations ante to filing a claim, but could instead proceed by instigating an individual adjudication. In essence, the determination of method of notice to those that an agency regulates is under plenary authority to the agency. In June 2014, the same court ruled that the hotel conglomerate could seek interlocutory review of portions of the opinion mentioned above.[164] It reasoned that

161. 10 F. Supp. 3d 602 (D.N.J. 2014).
162. According to the FTC, these breaches led to the compromise of more than 619,000 consumer payment card account numbers, numbers that were exported to a domain registered in Russia. The affected consumers also suffered more than $10.6 million in fraud loss as a result of the breach.
163. See Brown & Williamson, 529 U.S. 120 (2000) (noting that it was clear that Congress intended to exclude tobacco products from the FDA's jurisdiction). The court contrasted this illustration of Congressional intent with the fact that all of the statutes dealing with data privacy, e.g., the FCRA, GLBA, COPPA, and HIPPA, actually complemented, if not granted, the authority of the FTC to regulate under the unfairness prong of the Act.
164. See FTC v. Wyndham Worldwide Corp., No. 2:13-cv-01887-ES-JAD (D.N.J. June 23, 2014). The relevant statute for interlocutory review is 29 U.S.C. § 1292(b); see also Litgo, NJ Inc v. Martin, 2011 WL 1134676 (D.N.J. Mar. 25, 2011) ("The burden is on the movant to demonstrate that all three requirements are met.").

    The controlling questions of law sufficient to trigger an interlocutory appeal were: (1) whether the FTC can bring an unfairness claims involving data security under Section of the FTC Act and (2)whether the FTC must formally promulgate regulations before bringing its unfairness claim under Section 5 of the FTC Act.

because there were controlling questions of law with substantial grounds for a difference of opinion, an interlocutory appeal "may materially advance the ultimate termination of the litigation."

- **In re ScanScout, Inc. –** An online advertiser agreed to settle FTC charges that it deceptively claimed that consumers could opt out of receiving targeted ads by changing their browser settings to block cookies, when in fact, the advertiser used Flash cookies that couldn't be blocked by browser settings.[165] The proposed settlement, among other things, bars misrepresentations about the company's data-collection practices, and requires that the advertiser provide a user-friendly mechanism to allow consumers to opt out of being tracked, including the use of a hyperlinked, embedded within or immediately next to its targeted display ads, to take consumers to a choice mechanism where consumers can opt out of receiving targeted ads.
- **In re Blue Cross Blue Shield of Tennessee –** A healthcare insurer agreed to pay a civil fine of $1,500,000 to settle certain HIPAA violations stemming from the theft of 57 unencrypted computer hard drives that contained the protected health information of over a million individuals.[166] According to HHS allegations, the insurer failed to implement appropriate administrative safeguards to adequately protect data servers remaining at a unused, leased facility by not performing the required security evaluations and implementing appropriate physical protections as required by the HIPAA Security Rule. Notably, this was the first enforcement action under the data breach rules mandated by the HITECH Act.

---

165. In re ScanScout, Inc., FTC File No. 1023185 (Settlement announced Oct. 8, 2011). See also United States v. Rental Research Services, Inc., No. 09-00524 (D. Minn. settlement announced Mar. 5, 2009) (consumer reporting agency that failed to properly screen prospective customers and, as a result, sold multiple credit reports to identity thieves, settled FTC charges that it violated the Fair Credit Reporting Act); In re Genica Corp., FTC File No. 082 3113 (settlement announcement Feb. 5, 2009) (online computer seller that collected sensitive information from consumers and allegedly failed to take basic security measures settled FTC charges); United States v. Central Florida Investments, Inc., No. 09-104 (M.D. Fla. Jan. 20, 2009) (company that called consumers whose phone numbers were on the Do Not Call Registry without consent or an "established business relationship" settled FTC charges that it violated the Do Not Call Registry provisions).
166. In re Blue Cross Blue Shield of Tennessee (HHS Settlement announced Mar. 13, 2012).

- **United States v. W3 Innovations** In the agency's first case involving smartphone apps, an iPhone app developer settled FTC charges that it violated COPPA by improperly collecting and disclosing personal information from tens of thousands of children under age 13 without their parents' prior consent.[167] The FTC complaint charged that the developer's children-oriented apps allowed children to post personal information on message boards without first obtaining parental consent. Under the terms of the consent decree, the developer was obligated to pay a $50,000 penalty, follow the COPPA Rule in the future and delete all personal information from users collected in violation of the Rule.

Computer Fraud and Abuse Act

Among other things, the Computer Fraud and Abuse Act (CFAA)[168] prohibits accessing a computer and obtaining information "without authorization" or by "exceeding authorized access." The statute lists many different types of criminal "hacking" conduct punishable by fines or imprisonment. In relevant part, §1030(a)(2)(C) provides: "[Whoever] intentionally accesses a computer without authorization or exceeds authorized access and thereby obtains…information from any protected computer if the conduct involved an interstate or foreign communication…shall be punished," and in related statutory language, §1030(a)(4) prohibits similar behavior with an intent to defraud.

- **United States v. Auernheimer** – In a recent case, the Court of Appeals for the Third Circuit confronted a situation in which a hacker was charged in a District Court in New Jersey with a conspiracy to commit an "ordinary violation" of the CFAA under 18 U.S.C. § 1030(a)(2)(C) and (c)(2)(B)(ii).[169] The "ordinary

---

167. United States v. W3 Innovations, LLC, No. 11-03958 (N.D. Cal. Consent Decree Aug. 12, 2011). See also United States v. Path, Inc., No. 13-0448 (N.D. Cal. settlement announced Feb. 1, 2013) (app operator agreed to settle FTC charges that it deceived users by collecting personal information from their mobile address books without consent and that it illegally collected personal information from children without their parents' consent; settlement required operator to pay a civil fine, establish a comprehensive privacy program and obtain independent privacy assessments every other year for the next 20 years).
168. 18 U.S.C. §1030 et seq.
169. 748 F.3d 525 (3d Cir. 2014). Auernheimer was also charged with conspiring to violate the CFAA in furtherance of a state crime under 18 U.S.C. § 1030 (c)(2)(B). He was accused of violating N.J. Stat. Ann. § 2C:20-31(a) which proscribes accessing a computer or computer system in excess of authorization

violation" involved the defendant's decision to hack into AT&T website via knowledge of the iPad user IDs and steal nearly 114,000 email addresses from its databases. This claim was essentially defeated on procedural grounds, as two of the "essential conduct" elements of a CFAA violation: (1) accessing without authorization; and (2) obtaining information, did not occur in the state in which the defendant was charged.[170] Specifically, the servers accessed were located in Texas and Georgia and defendant Auernheimer was located in Arkansas, thus "no protected computer was accessed and no data was obtained in New Jersey." Likewise, there was no evidence that the personal data disclosed to a reporter occurred when the reporter was in New Jersey. Therefore, the conviction was overturned on grounds of improper venue.[171]

- **United States v. Nosal** – Under the criminal provisions of the CFAA, a departing employee who accessed his employer's databases to help start a competing business did not "exceed authorized access" of the computer system even if such use of the proprietary materials violated the employer's computer use policy.[172] The Ninth Circuit, sitting en banc, affirmed the lower court's dismissal of the criminal CFAA claim and rejected the

---

that "discloses or causes to be disclosed any data … or personal identifying information." Such charge was dismissed on grounds of improper venue, as discussed *infra*.

170. See also United States v. Willis, 476 F.3d 1121 (10th Cir. 2007) (delineating the CFAA elements). Further, the court noted the distinction between "essential conduct" elements from "circumstance element[s]" in the context of conspiracy charges. See United States v. Rodriguez-Moreno, 526 U.S. 275 (1999).
171. The court noted that "[a]lthough this appeal raises a number of complex and novel issues that are of great public importance in our increasingly interconnected age, we find it necessary to reach only one that has been fundamental since our country's founding: venue. 748 F.3d at 532; see also United States v. Cabrales, 524 U.S. 1 (1998) (noting that the Constitution "twice safeguards the defendant's venue right").
172. United States v. Nosal, 676 F.3d 854 (9th Cir. 2012) (en banc). See also WEC Carolina Energy Solutions LLC v. Miller, 687 F.3d 199 (4th Cir. 2012) (CFAA fails to provide a remedy for misappropriation of trade secrets or violation of a use policy where authorization has not been rescinded (citing *Nosal*); based on the ordinary meaning of "authorization," an employee is authorized to access a computer when his employer approves or sanctions his admission to that computer and acts "without authorization" when he gains admission to a computer without approval; similarly, an employee "exceeds authorized access" when he has approval to access a computer, but uses his access to obtain or alter information that falls outside the bounds of his approved access; neither of these definitions extends to the improper use of information validly accessed).

Government's broad interpretation of the CFAA that would have "transform[ed] the CFAA from an anti-hacking statute into an expansive misappropriation statute." The court held that the language "exceeds authorized access" in the CFAA is limited to violations of restrictions on "access" to information, and not restrictions on its "use," that the statute targets "the unauthorized procurement or alteration of information, not its misuse or misappropriation." Clarifying the two-prongs of the CFAA's prohibitions, the court stated: "'[W]ithout authorization' would apply to *outside* hackers (individuals who have no authorized access to the computer at all) and 'exceeds authorized access' would apply to *inside* hackers (individuals whose initial access to a computer is authorized but who access unauthorized information or files)." Construing the criminal statutory language narrowly, the appeals court found that a broad interpretation of the CFAA would turn minor online dalliances by employees using company computers into federal crimes and that significant notice problems would arise if criminal liability turned on the vagaries of corporate computer use polices that are lengthy, opaque, subject to change and seldom read.

- **United States v. John** – In contrast to *Nosal*, the Fifth Circuit upheld a criminal conviction under the CFAA after an employee had used her employer's computer to obtain confidential customer information, despite the employee having authorization to access such information.[173] The defendant argued that she was allowed to use her employer's computers to view and print confidential information regarding customer accounts and was only forbidden from using the information to which she had access to perpetuate a fraud. Specifically, the court held that the CFAA may encompass limits on *the use of information* obtained by permitted access to a computer system and the data on that system. Therefore, an individual could "exceed authorized access" under the CFAA simply based on misuse of information gleaned from such access. With respect to the language in the CFAA pertaining to accessing a computer "without authorization," the court applied the "intended-use analysis" to conclude that, although the defendant had authorization to view and print all of the confidential information she accessed, such use to perpetuate fraud was not *an intended use of*

173. 597 F.3d 263 (5th Cir. 2010).

that system."[174] Finally, the Fifth Circuit noted that the defendant's use of the employer's computer system violated the employer's employee policies, of which she was aware. It cited to another circuit in holding that an "employment agreement can establish the parameters of authorized access."

- **United States v. Drew** – A misdemeanor violation under the 18 U.S.C. §§ 1030(a)(2)(C) and 1030(c)(2)(A) of the CFAA upon the conscious violation of a website's terms of service runs afoul of the void-for-vagueness doctrine because of the absence of minimal guidelines to govern law enforcement and actual notice deficiencies.[175] The court granted the defendant's motion for a post-verdict acquittal and vacated her CFAA misdemeanor conviction. The court commented that the concept of accessing a computer "without authorization" usually involved a computer hacker, a disloyal employee accessing proprietary files, or The defendant argued that she was allowed to use her employer's computers to view and print confidential information regarding customer accounts and was only forbidden from using the information to which she had access to perpetuate a fraud.an entity in breach of a contract. Within the breach of contract approach, the court determined that most judges, in the civil law context, have held that a conscious violation of a website's terms of service will render the access unauthorized and/or cause it to exceed authorization. It cannot be considered "a stretch of the

174. Id. at 271-72. The court cited to *United States v. Phillips*, a case in which the same court concluded that "without authorization" in the context of the CFAA is "typically analyzed" with respect to the "scope of a user's authorization to access a protected computer on the basis of the expected norms of intended use or the nature of the relationship established between the computer user." 477 F.3d 215 (5th Cir. 2007).

175. United States v. Drew, 259 F.R.D. 449 (C.D. Cal. 2009). See also United States v. Aleynikov, 2010 WL 3489383 (S.D.N.Y. Sept. 03, 2010) (government's argument that defendant, who was authorized to access his employer's trading system source code, violated the criminal provisions of the CFAA by misappropriating the source code was rejected), *reversed on other grounds*, 676 F.3d 71 (2d Cir. 2012) (conviction under federal EEA overturned because, among other things, the wrongful uploading of his employer's proprietary source code did not implicate a system that was "produced for" or "placed in" interstate or foreign commerce); United States v. Zhang, 2012 WL 1932843 (N.D. Cal. May 29, 2012) (applying the Ninth Circuit's holding in *Nosal*, departing employee who misappropriated confidential information in violation of nondisclosure agreement did not exceed authorized access and was not guilty of CFAA charges; defendant convicted for theft of trade secrets under federal law).

law to hold that the owner of an Internet website has the right to establish the extent to (and the conditions under) which members of the public will be allowed access," according to the court. However, the court stated that individuals of "common intelligence" are arguably not on notice that a breach of a terms of service contract can become a crime under the CFAA. Notably, the court reasoned that if a website's terms of service controls what is "authorized" and what is "exceeding authorization" – which in turn governs whether an individual's conduct is criminal or not – the statute would be unacceptably vague because "it is unclear whether any or all violations of terms of service will render the access unauthorized, or whether only certain ones will."

Although principally a criminal statute, the CFAA also provides for a private civil right of action, allowing for awards of damages and injunctive relief in favor of any person who suffers a loss due to a violation of the act. Although the CFAA was enacted almost 25 years ago, courts continue to decide how the statute applies to new factual scenarios in a rapidly and ever-changing computerized world.

- **Craigslist Inc. v. 3Taps Inc. –** A website operator who revoked access under the "without authorization" provision in the CFAA for a previously authorized user will not have those actions struck down on a motion to dismiss.[176] In the case, the plaintiff, a popular website operator, brought an action against a one of its previously authorized users under the CFAA's mandate forbidding users to access a website "without authorization." In rejecting defendant's motion to dismiss, the court agreed with the plaintiff that interpreting the "without authorization" provision of the CFAA according to the plain language of the statute would permit the revocation of previously granted access. Namely, the court noted that "without authorization" possessed an "unambiguous and plain meaning" as referring to an authorization emanating from "permission or power granted by an authority." Accordingly, since the plaintiff in the case had explicitly revoked the access via both a cease-and-desist letter and through technological means, the defendant could not claim that their continuing access did not constitute access "without authorization" pursuant to the CFAA.[177] The court similarly

176. Craigslist Inc v. 3Tapas Inc, 964 F. Supp. 2d 1178 (N.D. Cal. 2013).
177. In order to prevent the defendant from accessing the site, Craigslist had configured its website to block IP addresses associated with it. In response, the defendant

rejected the argument by the defendant, as discussed extensively in *Nosul*, that holding for the plaintiff could criminalize a wide swath of user conduct based on use policies. The court distinguished the instant case from *Nosul* primarily on the grounds that the defendant was completely blocked from accessing Craigslist, and therefore did not have any legitimate grounds to "use" the site at all, and thus could not claim that the restrictions placed on it was in reference to their usage of the site, as opposed to their access.[178]

- **Cassetica Software, Inc. v. Computer Sciences Corp.** – The unauthorized downloading of software from a computer system after a licensing agreement had expired does not satisfy the "damage" element under the Computer Fraud and Abuse Act (CFAA) because the statute only recognizes damage when the violation causes a diminution in the completeness or usability of the data on a computer system.[179] The court found that the plaintiff failed to allege that the defendant's downloads resulted in lost data, the inability to offer downloads to its customers, or that the downloads affected the availability of the software. The court also found that the plaintiff's allegations of "loss" was not cognizable because they were costs that were not related to the impairment or damage to a computer or computer system.

Most notably, the CFAA has been used increasingly in civil suits by employers to sue former employees and their new companies

---

had continued to access Craigslist by using different IP addresses and proxy servers, thereby in part necessitating the decision by Craigslist to litigate.

178. Craiglist, 2013 WL 4447520, at *5. The defendant also argued that Craiglist was labeling an access restriction what was in actuality a use restriction. Only the latter implicates the issues discussed in *Nosul* concerning the criminalization or restriction of user internet freedom based on policies that said user likely has minimal knowledge of the existence of at all. The court disagreed in noting that, according to the facts of the case, Craiglist was issuing a blanket restriction on access for defendant, a restriction not subject to caveats or carve outs depending on the type of use defendant wished to undertake. Specifically, the court stated that the defendant in the case had one unequivocal restriction on its conduct: do not access the website. See also Wentworth-Douglass Hosp. v. Young & Novis Prof'l Ass'n, No. 10–CV–120–SM, 2012 WL 2522963, at *4 (D. N.H. June 29, 2012) ("[S]imply denominating limitations as access restrictions does not convert what is otherwise a use policy into an access restriction.") (internal quotations omitted).

179. Cassetica Software, Inc. v. Computer Sciences Corp., 2009 WL 1703015 (N.D. Ill. June 18, 2009).

for misappropriation of information from the employer's computer system, beyond the standard state causes of action for trade secret misappropriation and breach of contract. A civil cause of action under the CFAA frequently is pleaded in cases where an employer is suing a former employee for misappropriation of trade secrets or proprietary information, where the misappropriation involved some kind of access to or use of the employer's computer network. However, federal courts disagree in interpreting the term "unauthorized access." Under an expansive view, courts have found that an employee's access was unauthorized after she engaged in conduct which could constitute a breach of her duty of loyalty to the company. Taking a narrower reading of the statute, many courts have found that a departing employee, who copied proprietary files while still having full access to his employer's protected computer databases, did not access information "without authorization" or otherwise "exceed authorized access" under the CFAA.[180]

- **LVRC Holdings, LLC v. Brekka** – A departing employee who emailed certain company documents to his own personal computer before departure did not access the computers "without authorization" or in excess of "authorized access" as required under the CFAA to establish a violation.[181] The appeals court affirmed the

180. See also Flynn v. Liner Grode Stein Yankelevitz Sunshine Regenstreif & Taylor LLP, 2011 WL 2847712 (D. Nev. July 15, 2011) (aiding and abetting civil liability does not exist under §1030).

181. LVRC Holdings, LLC v Brekka, 581 F.3d 1127 (9th Cir. 2009). See also ReMedPar Inc. v. AllParts Medical LLC, 683 F. Supp. 2d 605 (M.D. Tenn. 2010) (CFAA does not extend to situations where the employee's access was technically authorized but the particular use of the information was not; also, the employer's "loss" at issue (i.e., the misappropriation of trade secret information) as well as the costs incurred by the employer in its efforts to seek redress for those acts and retain new employees are not the type of losses covered by the statute because they are unrelated to any interruption in computer service); Orbit One Communications, Inc. v. Numerex Corp., 692 F. Supp. 2d 373 (S.D.N.Y. 2010) (departing employees had unfettered access to employer's computers prior to leaving the company and thus plaintiff-employer failed to advance any evidence that the departing employees accessed the plaintiff's computer system without authorization or exceeded their authorized access in violation of the CFAA); Oce North America Inc. v. MCS Services Inc., 748 F.Supp.2d 481 (D. Md. 2010) (ex-employee who allegedly copied printer diagnostic software from his ex-employer and used it during his work for a competitor did not access the software "without authorization" under the CFAA; CFAA claims against the employee's new employer were also dismissed because the plaintiff did not allege that the defendant accessed any "protected computer" without authorization or in excess of that authorization to obtain the plaintiff's software); Advanced Aerofoil Technologies AG v. Todaro,

dismissal of the CFAA claims against the ex-employee. The court found that a person uses a computer "without authorization" when the person has not received permission to use the computer for any purpose (e.g., a hacker) or when the employer has rescinded permission to access the computer and the employee thereafter accesses the company network. In this case, the court concluded that the employee's use of the company computers to email documents did not violate the CFAA because he was authorized to access the company computers during his employment. The court reasoned that there was no language in the CFAA that supported the proposition that authorization to use a computer ceases when an employee resolves to use the computer contrary to the employer's interest. The court declined to follow the Seventh Circuit decision, *International Airport Centers, LLC v. Citrin*,[182] which held that an employee acts without authorization under the CFAA when he obtains company information for an improper purpose.

- **TelQuest Int'l Corp. v. Dedicated Business Systems, Inc.** – Departing employees who allegedly violated a non-competition employment agreement and used private customer information to initiate their own business did not violate the CFAA because the employer failed to allege facts that the damage or loss it incurred was related to investigating or remedying damage to its computer system.[183] The court dismissed the employer's CFAA claims. The

---

2013 WL 410873 (S.D.N.Y. Jan. 30, 2013) ("because there is no allegation that [the plaintiff-employer] revoked Defendants' unlimited access to its system, Plaintiffs cannot state a cognizable claim under the CFAA"); JBCHoldings NY, LLC v. Pakter, 2013 WL 1149061 (S.D.N.Y. Mar. 20, 2013) (employee's misuse of an employer's proprietary data does not violate the CFAA where the information was obtained from a computer to which the employee was permitted access).

182. 440 F.3d 418 (7th Cir. 2006).

183. TelQuest Int'l Corp. v. Dedicated Business Systems, Inc., 2009 WL 3234226 (D. N.J. Sept. 30, 2009). See also Catapult Communications Corp. v. Foster, 2010 WL 3023501 (N.D. Ill. July 30, 2010) (alleged losses in the form of expenses incurred from conducting forensic analysis on defendant's computer are not compensable losses under the CFAA, without any evidence that plaintiffs' computers were damaged by defendant's alleged unauthorized access); General Scientific Corp. v. Sheervision, Inc., 2011 WL 3880489 (E.D. Mich. Sept. 2, 2011) (losses under the CFAA are limited to costs incurred and profits lost as a direct result of interrupted computer service; the CFAA's damage requirement is not concerned with sales lost through the use of the information accessed); Schatzki v. Weiser Capital Management LLC, 2012 WL 2568973 (S.D.N.Y. July 3, 2012) (plaintiffs' claim inadequate to meet the definition of damages and losses under the CFAA; the complaint does not allege that the defendant, a former business

court found that the employer allegations regarding losses related to hiring a computer expert failed to provide the type of investigation or description of how its computer system was interrupted, damaged, or restored. The court also commented that gathering evidence from a computer to prove state law employment claims does not turn employee conduct–even allegedly disloyal conduct in breach of contract–into the kind of conduct that violates the CFAA.

Beyond federal law, a majority of states have enacted computer trespass and fraud statutes that allow claims for various degrees of unauthorized access and copying, schemes to defraud, and the unlawful destruction of proprietary data.

- **Joseph Oat Holdings Inc. v. RCM Digesters Inc. –** An entity who secretly accessed the servers of its former business partner, copied proprietary files and changed administrative passwords following the dissolution of the parties' joint venture violated California and New Jersey state computer trespass laws.[184] The court granted summary judgment on defendant's computer trespass counterclaims, holding that at the time the plaintiff accessed the defendant's computer server (which had formerly been used by the joint venture), the server had reverted back to the property of the defendant because the joint venture had been officially defunct. The court rejected the plaintiff's argument that it copied the defendant's files to preserve evidence pursuant to a litigation hold letter, finding that an adversary's counsel's letter regarding the duty to preserve evidence does not "afford a party carte blanche authority" to secretively copy computer files located on the adversary's computer server, even if many of those files on the server had once been property of that party, and even if that party still had access to those files.

---

partner, destroyed or impaired the plaintiff's proprietary data, nor does it make any specific allegation as to the cost of identifying, securing or remedying the alleged damage caused by the defendant's access).

184. Joseph Oat Holdings Inc. v. RCM Digesters Inc., 2009 WL 3334868 (D. N.J. Oct. 14, 2009).

Commercial Email and Spam

The CAN-SPAM Act,[185] which imposes requirements on those who send commercial email messages to consumers and establishes civil and criminal penalties for the transmission of unsolicited commercial electronic mail, or spam, that does not comport with the Act's requirements, continues to garner the public's attention as spam remains a stubborn problem. Essentially, the CAN-SPAM Act protects consumers by offering them a legal right to "opt out" of future spam. In most situations, it is not required that a business get permission from a potential recipient before sending commercial email. Still, businesses are not permitted to send commercial emails to those who request to be removed from the businesses' lists

Notably, the act expressly preempts all state laws to the extent that they address the permissibility of unsolicited commercial email, except for those that apply "falsity or deception in any portion of a commercial electronic mail message or information attached thereto." Courts have wrestled with the question of what constitutes falsity or deception under the statute, whether cognizable state claims must be based on the traditional tort theory of common law fraud and deceit, which usually requires a plaintiff to plead it with particularity, or whether state consumer or anti-spam laws may survive preemption for regulating something less than fraud. District courts to have addressed the issue have reached differing results

- **Facebook, Inc. v. Maxbounty, Inc. –** The CAN-SPAM Act applies to social networking communications–including internal messages to users' walls, "news feeds," the "home" page of users' friends, and the Facebook inbox of users' friends–despite the fact that such electronic messages are not delivered to a traditional email "inbox."[186] The court refused to dismiss the plaintiff's CAN-SPAM claims against an Internet marketer that had allegedly set up fraudulent fan pages through its affiliates to draw traffic to outside sites and advertisers through a series of messages and notifications to Facebook users. The court rejected the defendant's argument that an "electronic mail message" under the CAN-SPAM Act must be capable of characterization as "email" or must be

185. Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, Pub L. No. 108-187, codified at 15 U.S.C. §7701.

186. Facebook, Inc. v. Maxbounty, Inc., 2011 WL 1120046 (N.D. Cal. Mar. 28, 2011).

directed to a traditional email inbox or address with a local part and domain part (i.e. user@domain.com).

- **Gordon v. Virtumundo, Inc. –** A provider of free email accounts for a small number of individuals who took no steps to stem the flow of spam emails does not have standing to pursue claims under the CAN-SPAM Act as a result of unsolicited commercial email sent to its users.[187] The appeals court affirmed the lower court's grant of summary judgment to the defendant and also ruled that the plaintiff's state anti-spam claims were preempted by the CAN-SPAM Act. The court held that the plaintiff was not a "provider of an Internet access service" who was adversely affected by a statutory violation and thus did not have private standing to bring CAN-SPAM Act claims. While the court recognized that statutory standing was not limited to traditional ISPs (and included providers such as social network websites), the court rejected any overly broad interpretation of "Internet access service" (IAS) that would include an entity that merely provided email accounts and email access. The court commented that the plaintiff neither had physical control over nor access to the hardware at issue, which was owned by another provider, and was "troubled" by the extent to which the plaintiff failed to operate as a "*bona fide* email provider," such that the plaintiff purposefully avoided taking even minimal efforts to

187. Gordon v. Virtumundo, Inc., 575 F.3d 1040 (9th Cir. 2009). See also Asis Internet Services v. Azoogle.com, Inc., 2009 WL 4841119 (9th Cir. Dec. 2, 2009) (unpublished) (mere cost of ordinary filtering and carrying spam over plaintiff's facilities does not constitute a harm as required by the CAN-SPAM Act; plaintiff did not suffered a harm within the meaning of the statute and lacked standing.), *further proceedings at* Asis Internet Servs. v. Optin Global, Inc., 2010 WL 2035327 (N.D. Cal. May 19, 2010) (defendant awarded attorney's fees in the amount of $806,978.84); RJ Production Co. v. Nestle USA, Inc., 2010 WL 1506914 (D.D.C. Apr. 15, 2010) (digital media outsourcing and consulting firm that made no allegations that it was an Internet access service that suffered any network harms lacked standing under the CAN-SPAM Act); but see Zoobuh Inc. v. Better Broadcasting LLC, 2013 WL 2407669 (D. Utah May 31, 2013) (bona fide online service that was adversely affected by spam had standing under the CAN-SPAM Act; in granting default judgment against the defendant, the court found false header violations based upon the defendant's use of a proxy service that displayed generic "From" names such that recipients could not readily trace back the spam email to the actual sender, and the court found Required Content violations because basic opt-out information was only displayed in a remotely hosted image, which was not likely to appear on the recipient's screen or otherwise be noticeable to the ordinary consumer).

avoid or block spam messages and accumulated spam through a variety of means for the purpose of facilitating litigation. As to the "adversely affected" standing requirement, the court stated that the fact that the plaintiff received a large volume of commercial email was not enough to establish his statutory standing. Rather, the court found that a plaintiff must plead those types of harms uniquely encountered by IAS providers, that is, network crashes, higher bandwidth utilization, and increased costs for hardware and software upgrades, network expansion and additional personnel, such that, in most cases, "evidence of some combination of operational or technical impairments and related financial costs attributable to unwanted commercial email would suffice." Interestingly, the appeals court noted that trial courts must take a closer look at services that may not be *bona fide* providers and "be careful to distinguish the ordinary costs and burdens associated with operating an Internet access service from actual harm," and that courts should also expect a legitimate service provider to "secure adequate bandwidth and storage capacity and take reasonable precautions, such as implementing spam filters, as part of its normal operations."

- **Ferguson v. Active Response Group** – An Internet access service provider that offers free email forwarding services lacks standing under the CAN-SPAM Act because he was not "adversely affected" by incoming spam when he was forced to switch to a broadband connection.[188] The appeals court affirmed the district court's grant of summary judgment to the defendant-online marketing company because the plaintiff failed to prove more than negligible harm due to the spam, such as increased costs for server maintenance, network harm, or for customer service personnel to handle complaints.

188. Ferguson v. Active Response Group, 2009 WL 3229301 (9th Cir. Oct. 8, 2009) (unpublished). See also Haselton v. Quicken Loans Inc., 2010 WL 1180353 (W.D. Wash. Mar. 23, 2010) (website host that attempted to grow a spam business and did not use any e-mail filtering programs was not bona fide IAS provider and accordingly lacked standing to pursue a claim under the CAN-SPAM Act; in addition, the plaintiff did not show it was "adversely affected" by any alleged violation of the CAN-SPAM Act since it suffered harm, if at all, by its own failure to implement spam reducing measures and its actions to actively seek out such communications).

Telephone Consumer Protection Act

The Telephone Consumer Protection Act (TCPA) was originally adopted in 1991 to, among other things, protect the privacy of citizens by restricting the use of telephones for unsolicited advertising and, more specifically, curb telemarketers from using autodialers to make millions of unsolicited calls to residential and business telephone numbers, fax machines and cellular telephones. The TCPA also prohibits the use of any fax machine, computer, or other device to send unsolicited fax advertisements, absent certain consent requirements.

- **Gomez v. Campbell-Ewald Co.** – In another case at the Ninth Circuit dealing with the intersection between the TCPA and SMS text messages, the court held in 2014 that the TCPA as applied to such messages does not violate the First Amendment.[189] In *Gomez v. Campbell-Ewald Co.*, the defendant that had sent an unsolicited text message to the plaintiff advocating a career in military service argued that the TCPA was unconstitutional as applied to SMS text messages. The court rejected this argument in noting that because the restrictions were constitutional insofar as the protection of privacy is a significant interest, and the restrictions in the TCPA to effectuate such protection were narrowly tailored and allowed for many alternative channels of communication.[190] The defendant had argued that the TCPA extended solely to the protection of residential privacy, and therefore since SMS text messages were often sent to phones while a user was not at home, the TCPA could thus categorically be inapplicable. Even when presupposing that the TCPA was limited to the government's significant interest in residential privacy, the "nature of cell phones" renders the restriction of unsolicited SMS text messages all the more necessary since

189. 768 F.3d 871 (9th Cir. 2014).
190. Id. (citing Moser v. FCC, 46 F.3d 970 (9th Cir. 1995)). Moser affirmed the notion that the government may impose reasonable restrictions (in this instance, via the TCPA) on the time, place, or manner of protected speech as long as the restrictions were not a reference to the content of the speech, were narrowly tailored and left ample alternative channels of communications. See also Ward v. Rock Against Racism, 491 U.S. 781 (1989); Clark v. Cmty. For Creative Non-Violence, 468 U.S. 288 (1984).

nearly all users have their cell phones with them while at home.[191]

- **Satterfield v. Simon & Schuster** – The transmission of an SMS text message to a cellular telephone is a "call" within the meaning of the Telephone Consumer Protection Act (TCPA).[192] The court reversed the district court's grant of summary judgment to the defendant and remanded the case to determine if the text message at issue was sent using an "automatic telephone dialing system" as required under the statute, that is, whether the equipment used for transmission had the "capacity" to both (1) store or produce numbers to be called using a random or sequential number generator and (2) to dial such numbers. The court found that the TCPA's prohibition on certain automated calls to wireless numbers encompasses both voice calls and SMS text messages, deferring to the FCC's regulations and interpretation of the Act and the plain meaning of the term "call." The court reasoned that the purpose and history of the TCPA indicated that Congress was trying to prohibit the use of automatic dialers to communicate with others by telephone in an invasive manner, and that a voice message or a text message were not distinguishable in terms of being an invasion of privacy. The court further held that while the TCPA

191. Moreover, it noted that since mobile phones are now the exclusive phone in many households, limiting calls to land lines alone would not "adequately safeguard the stipulated interest in residential privacy." See also Karen Kaplan, Still have a land line? 128 million don't, L.A. Times (July 8, 2014), http://www.latimes.com/science/sciencenow/la–sci–sn–wireless–only–householdsin–america–20140708–story.html.

192. Satterfield v. Simon & Schuster, 569 F.3d 946 (9th Cir. 2009). See also In re Jiffy Lube International, Inc., Text Spam Litigation, 2012 WL 762888 (N.D. Cal. Mar. 9, 2012) (advertiser not permitted to avoid TCPA liability merely because it hired a different firm to send text message advertisements to its customers); Hurst v. Mauger, 2013 WL 1686842 (N.D. Ill. Apr. 16, 2013) (e-commerce service provider and payment processor not liable under TCPA for seller's spam text messages; the fact that provider earned a commission from the sale of the seller's products did not conclusively establish that the messages were sent "on behalf of" the provider, a fact bolstered by anti-spam provisions in the agreement between the provider and seller that cut against the suggestion that the provider played any role in the sending of the messages). But see Thomas v. Taco Bell Corp., 2012 WL 3047351 (C.D. Cal. June 25, 2012) (a party can be held liable under the TCPA directly if it personally "makes" a call in the method proscribed by the statute, or vicariously, such as, if it was in an agency relationship with the party that sent the text message; plaintiff failed to present any evidence that defendant directed or supervised the manner and means of the text message campaign conducted by an association of its franchisees).

exempts those calls "made with the prior express consent of the called party," no express consent was given in this case because the plaintiff's consent to receive promotional material from a third-party marketer and its "affiliates and brands," cannot be read as consenting to the receipt of the commercial messages of the defendant, an unrelated entity. This case was unequivocally reaffirmed five years later by the court in *Campbell-Ewald Co.*

- **Abbas v. Selling Source, LLC** – An unsolicited, commercial SMS message is a "call" within the meaning of the TCPA because Congress intended to restrict unsolicited, automated advertisements and solicitations by telephonic means, which includes text messages.[193] The court denied the defendant's motion to dismiss the defendant's TCPA claims. The court rejected the defendant's argument that the TCPA was inapplicable because there was no evidence that the plaintiff was "charged for the call," concluding that beyond "cost-shifting" concerns, Congress was just as concerned with consumers' privacy rights and the nuisances of telemarketing such that a cellular phone customer need not necessarily be charged for the call to make that call actionable.
- **Stern v. Bluestone** – Unsolicited, faxed "commentaries" containing short essays on legal topics in an attorney's field of practice that also list the sending attorney's law firm name and contact information fit the FCC's framework for an "informational message" and are not unlawful "unsolicited advertisements" under the TCPA.[194] The New York Court of Appeals reversed the lower

193. Abbas v. Selling Source, LLC, 2009 WL 4884471 (N.D. Ill. Dec. 14, 2009); but see Ryabyshchuck v. Citibank N.A., 2012 WL 5379143 (S.D. Cal. Oct. 30, 2012) (text message confirming opt-out request held non-actionable under the TCPA; "such simple, confirmatory response to plaintiff-initiated contact can hardly be termed an invasion of privacy under the TCPA); Ibey v. Taco Bell Corp., 2012 WL 2401972 (S.D. Cal. June 18, 2012) (advertiser's single, confirmatory text message in response to an opt-out request from plaintiff, who voluntarily had provided his phone number by sending the initial text message, does not violate the TCPA).
194. Stern v. Bluestone, 2009 NY Slip Op 04740 (N.Y. June 11, 2009). See also Holmes v. Back Doctors, Ltd, 2009 WL 3425961 (S.D. Ill. Oct. 21, 2009) (faxed newsletter that contained bona fide medical information that changed each month and was sent to specific recipients on a regular schedule does not constitute an "advertisement" under the TCPA; while the faxes contained some advertising material, "it is worth noting that the TCPA actually requires the sender of a fax to include its contact information in the fax…and the Court sees no reason why [defendant's] compliance with the statute should become…the linchpin for finding that [defendant's] faxes constitute advertising"); Holtzman v. Turza,

court's grant of summary judgment to the plaintiff on his TCPA claims. The court found that the defendant's commentaries, which provided academic legal information, did not promote a commercial product and to the extent that the defendant devised the commentaries as a way to advertise his expertise to other attorneys and gain referrals, the faxes contained at most, "[a]n incidental advertisement of his services, which [did] not convert the entire communication into an advertisement."

- **Burdge v. Association Health Care Mgmt. –** Certain regulatory violations of the TCPA fall outside the scope of private enforcement actions.[195] The court concluded that there was no private right of action for failure on the part of an automated telemarketing call to identify itself or provide its phone number since the enforcement of such identification requirements was within the province of state attorneys general and the Federal Communications Commission, and could not form the basis of a private enforcement action.

First Amendment Issues in Digital Content

The First Amendment's freedom of speech and the press provide protection for certain uses of content on the Internet or in a digital application and can limit rights of publicity in one's name or likeness for newsworthy and other purposes.[196] Moreover, in certain instances,

---

2010 WL 3076258 (N.D. Ill. Aug. 3, 2010) (faxed newsletters that contained editorial and promotional content that were ghostwritten and transmitted on attorney's behalf as part of a paid marketing campaign were deemed unsolicited advertisements under the TCPA), *further proceedings at* 2011 WL 3876943 (N.D. Ill. Aug. 29, 2011) (plaintiff granted summary judgment, with the court awarding $4,215,000 in damages, $500 in statutory damages for each of the 8,430 times faxes successfully sent to the class members).

195. Burdge v. Association Health Care Mgmt., 2009 WL 414595 (S.D. Ohio Feb. 18, 2009). See also Dobbin v. Wells Fargo Auto Finance, Inc., 10-268 (N.D. Ill. June 14, 2011) (recipients of cell phone calls failed to establish a genuine issue of fact regarding whether manually dialed calls made from a bank call center desk phone were made "using" equipment with the capacity to autodial within the meaning of the TCPA since such desk phones could be used independently of the predictive dialing technology employed by the bank); CE Design, Ltd. v. Prism Business Media, Inc., 2010 WL 2104272 (7th Cir. May 27, 2010) (the "established business relationship exception" to the TCPA's junk fax prohibitions applies to both business and residential customers).

196. See e.g., Nieman v. VersusLaw, Inc., 512 Fed. Appx. 635 (7th Cir. Mar. 2013) (privacy and right of publicity claims against legal search websites that linked to

students and public employees can be subject to restrictions in the name of school discipline and the objectives of a public employer. The First Amendment has also been invoked in placing limits on government restrictions on certain criminal's internet access[197] and in granting or limiting access to online records.[198]

- **FreeLife Int'l Inc. v. American Educational Music Publications, Inc.** – A non-disparagement clause contained in an online adhesion contract between a direct sales company and a prospective independent distributor is enforceable because it is neither procedurally nor substantively unconscionable and does not violate the First Amendment.[199] In ruling on the enforceability of the online contract's non-disparagement clause, the court found that the defendant completed the application and stated affirmatively that he accepted the terms and that the non-disparagement clause was not objectively bizarre or oppressive such that the adhering party "would not have assented to the particular term had he or she known of its presence." The court commented that the defendant accepted the contract with the non-disparagement clause and, now that he allegedly has breached it, cannot be heard to claim it is unfair because of the possible consequences of his breach. The court also rejected the defendant's First Amendment argument, stating that the First Amendment protects individuals from government infringement on speech, not private infringement.

---

court documents regarding a prior lawsuit in the plaintiff's name were barred by the First Amendment).

197. See e.g., Doe v. Prosecutor, Marion County, Indiana, 2013 WL 238735 (7th Cir. Jan. 23, 2013) (Indiana statute that prohibited most registered sex offenders from using social network websites and instant messaging services held unconstitutional because it was not narrowly tailored to serve the state's interest and broadly prohibited protected speech rather than specifically targeting the evil of improper communications to minors).

198. See e.g., In re Appelbaum, 2013 WL 286230 (4th Cir. Jan. 25, 2013) (no First Amendment right to access orders issued under SCA, 18 U.S.C. § 2703(d), at the pre-grand jury phase of the ongoing Wikileaks criminal investigation since there is a lack of First Amendment right to access such documents and the common law right to access such documents is outweighed by countervailing government interests); People v Harris, 36 Misc 3d 868 (N.Y. Crim. Ct. Sept. 11, 2012) (court refuses to quash district attorney's subpoena to Twitter to obtain subscriber information and tweets from protester; court found no expectation of privacy in public tweets and allowed release of non-content information under the SCA).

199. FreeLife Int'l Inc. v. American Educational Music Publications, Inc., 2009 WL 3241795 (D. Ariz. Oct. 1, 2009).

- **Estavillo v. Sony Computer Entertainment –** A user that was banned from the defendant's videogame network after multiple violations of its terms of use cannot state a plausible First Amendment claim for relief because the defendant was merely providing a private commercial product and did not have a sufficient structural or functional nexus to the government for the First Amendment to apply.[200]
- **Richerson v. Beckon –** The transfer of an education instructional coach to another position after it was discovered that she wrote a publicly-available blog that included several highly personal and vituperative comments about her employers and fellow teachers did not violate the instructional coach's First Amendment rights.[201] The court found that the legitimate administrative interests of the school district outweighed the plaintiff's First Amendment interests in not being transferred because of her speech, despite the fact that it arguably touched on matters of public concern.
- **Stengle v. Office of Dispute Resolution –** A state administrative hearing officer's termination due to her personal blog that addressed the same special education topics that she heard in her judicial capacity called did not violate her First Amendment or other civil rights.[202] The court granted the government agency's motion for

200. Estavillo v. Sony Computer Entertainment, 2009 WL 3072887 (N.D. Cal., Sept. 22, 2009). See also Stern v. Sony Corp., No. 09-7710 (C.D. Cal. Feb. 8, 2010) ("To the extent Plaintiff is suing Sony as a manufacturer of video games, and the provider of online services, Sony is not a "place of public accommodation" and is therefore not liable for violating Title III of the ADA").

201. Richerson v. Beckon, 2009 WL 1975436 (9th Cir. June 16, 2009) (unpublished). See also Yoder v. University of Louisville, 2012 WL 1078819 (W.D. Ky. Mar. 30, 2012) (nursing school that expelled student for making social media posting about a patient's birth did not violate her First Amendment rights; the school had a legitimate pedagogical purpose in requiring students to sign a confidentiality policy and the student "cannot now complain that she had a First Amendment right to publish on the internet the information she agreed not to reveal"), *aff'd* 2013 WL 1976515 (6th Cir. May 15, 2013).

202. Stengle v. Office of Dispute Resolution, 2009 WL 1138119 (M.D. Pa. Apr. 27, 2009). See also In re: Tenure Hearing of Jennifer O'Brien, 2013 WL 132508 (N.J. Super. Ct. App. Div. Jan. 11, 2013) (ALJ properly terminated teacher who wrote offensive Facebook posts about her students; court rejected First Amendment defense and agreed that comments were not matters of public concern and even if they were, her views were outweighed by the district's need to operate its schools efficiently); Zellner v. Herrick, 639 F.3d 371 (7th Cir. 2011) (teacher dismissal for violating computer use policy against viewing adult materials was warranted and unrelated to his outside union activities); Palleschi v. Cassano, 102 AD3d

summary judgment on the plaintiff's constitutional and civil rights claims, finding that her blog posed a legitimate threat to the efficient operation of the government agency such that the plaintiff's free speech rights as a government officer could be constitutionally abridged in these circumstances. The court stated that the plaintiff failed to show that her blogging activities had no potential to disrupt the governmental operations, particularly since her blog had the potential to induce recusal motions from those who came before her in her hearing officer capacity and encourage losing parties to question her impartiality following an adverse decision.

- **O.Z. v. Board of Trustees of Long Beach Unified School Dist. –** A school's transfer and discipline of student who created a slide show that was later posted on YouTube that depicted violence against a teacher was likely justified.[203] The court reasoned that

---

603 (N.Y. App. 1st Dept. 2013) (911 operator who photographed the computer screen showing the information surrounding an apparently humorous call and posted it on Facebook was properly terminated). But see Love v. Rehfus, 946 N.E.2d 1 (Ind. 2011) (firefighter was improperly terminated for sending a private email supporting a local political candidate to a small group of citizens because the email was constitutionally protected speech and there was little evidence suggesting the speech caused or had the potential to cause disruption or harm to the Fire Department's operations); Rubino v. City of New York, 2013 WL 1876235 (N.Y. App. Div., 1st Dept. May 7, 2013) (public school teacher's termination for tasteless Facebook posting about her students posted within her network of friends was not warranted where the petitioner had a long and otherwise unblemished employment history and expressed remorse).

203. O.Z. v. Board of Trustees of Long Beach Unified School Dist., 2008 WL 4396895 (C.D. Cal. Sept. 9, 2008). See also Kowalski v. Berkeley County Schools, 652 F.3d 565 (4th Cir. 2011) (student suspension over creation of MySpace page dedicated to ridiculing a fellow student did not violate the plaintiff's free speech rights because it was foreseeable that such conduct would reach the school via computers and smartphones and create a foreseeable substantial disruption there); D.J.M. v. Hannibal Public School District #60, 647 F.3d 754 (8th Cir. 2011) (suspension upheld where student sent violent threats over instant messenger program from his home); Harris v. Pontotoc County School Dist., 635 F.3d 685 (5th Cir. 2011) (school did not violate student's due process rights in suspending for causing a denial of service attack against the school network); Doninger v. Niehoff, 642 F.3d 334 (2d Cir. 2011) (school officials acted reasonably and deserved qualified immunity for prohibiting a student from running for Senior Class Secretary because of offensive off-campus blog posts that pertained to a school event); but see J.S. v. Blue Mountain School Dist., 650 F.3d 915 (3d Cir. 2011) (en banc) (school that suspended student for creating a lewd MySpace profile of the principal violated student's First Amendment rights because the facts simply do not support the conclusion that the School District could have reasonably

even if the student's posting was protected speech, it was reasonable, given the violent language and unusual photos depicted in the video slide show, for school officials to forecast substantial disruption of school activities.

TECHNOLOGY-RELATED PATENT LITIGATION

A patent represents the grant of a property right from the federal government to the inventor (or his assigns) for a limited time. The grant of this patent right represents a quid pro quo exchange between the inventor and the United States government. The inventor must disclose in his application a detailed description of how to make and use the new invention; in exchange for this full public disclosure of the invention and how it works, the government confers temporally limited rights of exclusivity on the inventor. Following the expiration of the exclusive term of the patent, the invention becomes part of the public domain, where the public may benefit from its disclosure by making, using, or selling the invention as it is described in the patent without permission from the patentee. In this way, the inventor's disclosure advances industry and furthers innovation. Importantly, the power of a patent does not oblige the patent holder to make, use, or sell the invention in his patent, but rather confers only the power to exclude others from doing so. What remedies a patent owner can be awarded in the instance of a successful infringement claim has become the subject of recent litigation at the Supreme Court level.

- **Octane Fitness, LLC v. ICON Health & Fitness, Inc.** – In 2014, the Supreme Court took up the issue of attorneys' fees awards in "exceptional" patent infringement cases.[204] In determining the standard for "exceptional cases," the Supreme Court abrogated the Federal

---

forecasted a substantial disruption of or material interference with the school as a result of fake social media profile created off-campus); Layshock v. Hermitage School Dist., 650 F.3d 205 (3rd Cir. 2011) (en banc) (student's suspension for creating fictitious, offensive social media profile of school official not justified under exceptions that allow punishment for off-campus behaviors); R.S. v. Minnewaska Area School Dist., 2012 WL 3870868 (D.Minn. Sept. 6, 2012) (First Amendment and privacy claims against school may proceed based upon search of student's Facebook account after a posting that was not truly threatening or disruptive to the school environment).

204. 134 S. Ct. 1749 (2014). In the case, since "exceptional" is not defined in the governing Patent Act, the Supreme Court construed it "in accordance with [its] ordinary meaning." See Sebelius v. Cloer, 133 S. Ct. 1886 (2013). It then listed a series of dictionary or previous case definitions that all centered around the words unusual, rare, not ordinary, uncommon, or special.

Circuit's test which required attorneys' fees only "when there has been some material inappropriate conduct related to the matter in litigation, such as willful infringement, fraud or inequitable conduct in procuring the patent, misconduct during litigation, vexatious or unjustified litigation … or like infractions."[205] In rejecting this test as "unduly rigid" and one that "impermissibly encumbers the statutory grant of discretion to district courts," the Supreme Court instead formulated a standard for attorneys' fee grants in patent litigation that is bereft of a "precise rule or formula," and that determines awards on a case-by-case basis. Specifically, attorneys' fees are granted in "exceptional" patent infringement when the case is one: that stands out from others with respect to the substantive strength of a party's litigating position (considering both the governing law and the facts of the case) or the unreasonable manner in which the case was litigated. As another rationale, the Supreme Court noted that to utilize the overly demanding Federal Circuit test would render the relevant Patent Act provision "largely superfluous," as no plaintiff would be able to satisfy such a high standard and thereby receive attorneys' fees, irrespective of the statutory provision permitting the acquisition of attorneys' fees in certain circumstances. Finally, the court held that the standard for determining attorneys' fees in "exceptional cases" was not "clear and convincing evidence," but a "simple discretionary inquiry."[206]

- **TransCore, LP v. Electronic Transaction Consultants Corp.** – A nonexclusive patent license is simply a promise not to sue for

205. For the principal case espousing this test, see Brooks Furniture Mfg., Inc v. Dutailier Int'l, 393 F.3d 1378 (Fed. Cir. 2005). The Brooks Furniture case also held that "[a]bsent misconduct in conduct of the litigation or in securing the patent," attorneys' fees "may be imposed against the patentee only if both (1) the litigation is brought in subjective bad faith, and (2) the litigation is objectively baseless." The Federal Circuit thereafter clarified that litigation is objectively baseless only if it is "so unreasonable that no reasonable litigant could believe it would succeed." See iLOR, LLC v. Google, Inc., 631 F.3d 1372 (Fed. Cir. 2011). Likewise, litigation is brought in "subjective bad faith" only if the plaintiff "actually know[s] that it is objectively baseless." Id. at 1377; see also Halo Electronics, Inc. v. Pule Electronics, Inc., 769 F.3d 1397 (Fed. Cir. 2014) (noting a change in the burden of proof for attorneys' fee shifting in patent cases).

206. See Octane Fitness, LLC v. ICON Health & Fitness, Inc., 134 S. Ct. 1749 (2014); see also Cooter & Gell v. Hartmarx Corp., 496 U.S. 384 (1990) (refusing to construe a similar fee-shifting statute to require proof of entitlement of fees by clear and convincing evidence); Bene v. Jeantet, 129 U.S. 683 (1889) (noting that patent infringement litigation has always been governed by a preponderance of the evidence standard).

infringement whether the agreement is framed in terms of a "covenant not to sue" or a "license" is merely a matter of form for the purposes of patent exhaustion.[207] The appeals court affirmed the dismissal of the patentee's infringement action against a downstream purchaser who acquired the claimed products from the patentee's competitor. The court found that a prior settlement agreement between the patentee and the competitor over earlier-issued patents was without apparent restriction or limitation and authorized all acts that would otherwise be infringements—making, using, offering for sale, selling, or importing—and as a result, the competitor's sales to the defendant were authorized and the patentee's rights were exhausted. Regarding the issue of legal estoppel, the appeals court stated that in order for the competitor to obtain the benefit of its settlement with the patentee, it must be permitted to practice not only the patents covered under the settlement agreement but also later-issued patents that are necessarily coextensive with the patents referenced in the agreement, such that the competitor became an implied licensee of the later-issued patent.

- **Wisconsin Alumni Research Found. v. Intel Corp.** – A software company's research grant to a university based upon contract language that gave the software company "unrestricted rights at no cost to the results of this research" did not give the software company the right to practice the hardware patent produced from the research.[208] In ruling in favor of the university, the court stated that the contract was ambiguous as to a grant of patent rights and held that given the circumstances underlying the agreement, the parties did not intend to transfer to the software company an express or implied license to the patent in exchange for the funding.
- **Quanta Computer, Inc. v. LG Electronics, Inc. –** The patent exhaustion doctrine prevents a patentee from further asserting its right in patented methods substantially embodied in products permissibly sold by its licensee to third-party downstream manufacturers.[209] The Supreme Court reversed the Federal Circuit's ruling that the patent exhaustion doctrine did not apply to method patents and held that the licensee's authorized sale of computer

207. TransCore, LP v. Electronic Transaction Consultants Corp., 563 F.3d 1271 (Fed. Cir. 2009).
208. Wisconsin Alumni Research Found. v. Intel Corp., 2009 WL 3003835 (W.D. Wis. Sept. 17, 2009).
209. Quanta Computer, Inc. v. LG Electronics, Inc., 128 S. Ct. 2109 (2008).

chipsets that substantially embody the method patents to the defendant-third-party manufacturer exhausted the plaintiff's patent rights. The Court held that the patent exhaustion doctrine applied to method claims; otherwise, patentees seeking to avoid patent exhaustion "could simply draft their patent claims to describe a method instead of an apparatus." The Court also found that the parties' licensing agreement, which required the licensee to give its customers notice that the patentee had not licensed those customers to practice its patents, did not, in fact, restrict the licensee's right to sell its products to downstream purchasers who intended to combine them with computer hardware not supplied by the licensee.

Congress has not enacted comprehensive patent law reform in more than 50 years. While Congress has considered patent reform legislation over the last decade, the need to modernize the patent laws has found expression in the courts as well. In recent years, the Supreme Court has reversed the Federal Circuit in at least a handful of patent-related cases. According to a Senate Judiciary Committee report, the Court's decisions have moved in the direction of improving patent quality and making the determination of patent validity more efficient, with the Court's decisions reflecting a growing sense that questionable patents are too easily obtained and are too difficult to challenge.

- **Leahy-Smith America Invents Act** – On September 16, 2011, the President signed patent reform legislation that amended the Patent Act in several important ways. Among other things, the patent reform law transitions the U.S. to a first-inventor-to-file patent system from a first-to-invent.[210] The first-to-file provisions become effective 18 months following passage of the law (i.e., March 16, 2013). Moreover, 18 months from the date of passage, the existing on sale bar will be eliminated, leaving a limited one-year grace period for certain disclosures made by the inventor (or joint inventor or by another who obtained the subject matter disclosed directly or indirectly from the inventor or a joint inventor). In addition, effective upon passage of the new law, an accused infringer may avoid liability by asserting a prior commercial use defense, which expands the defense to all areas of technology beyond business methods, and requires a showing of both reduction to practice and commercial use at least one year before the effective filing date of the claimed

210. Leahy-Smith America Invents Act, Pub.L. 112-29, 125 Stat. 284 (2011).

invention or the date on which the claimed invention was disclosed to the public in a manner that qualified for the exception from prior art under Section 102. See 35 U.S.C. §273(a). A person asserting the prior commercial use defense must establish it by clear and convincing evidence. The reform act also states that for accused infringers, the failure to disclose the best mode shall not be a basis on which any claim of a patent may be canceled or held invalid or otherwise unenforceable in cases filed after enactment.

- **Mayo Collaborative Servs. v. Prometheus Labs., Inc.** – Patent claims covering medical processes that helped doctors monitor the effects of certain medications based upon blood tests are unpatentable applications of natural laws under §101.[211] The Supreme Court reversed the Federal Circuit, which had held that the claimed medical treatment processes "transformed" human blood and satisfied the "machine or transformation" test. In a unanimous opinion, the Supreme Court found that the claimed processes were not patentable because they did not have additional features that provided practical assurance that the processes were genuine applications of those laws rather than drafting efforts designed to monopolize the correlations. The court stated that because methods for making such medical determinations were well known in the art, the patentee's claims simply told doctors to engage in well-understood, routine, conventional activity, and as such, were not sufficient to transform an unpatentable law of nature into a patent-eligible application of such a law. From a policy standpoint, the court reiterated its concern that patent law "not inhibit further discovery by improperly tying up the future use of laws of nature," particularly when a patented process "amounts to no more than an instruction to 'apply the natural law' or otherwise forecloses more future invention than the underlying discovery could reasonably justify." Notably, the court rejected the position adopted in the Government's amicus brief concerning the proper place of §101, stating that §101 was an established inquiry, and to shift the patent eligibility inquiry entirely to other patent law sections (e.g., §102 - novelty, §102 - obviousness, §112 - written description requirement) "risks creating greater legal uncertainty,

211. Mayo Collaborative Servs. v. Prometheus Labs., Inc., 132 S. Ct. 1289 (2012). See also Assoc. for Molecular Pathology v. Myriad Genetics, Inc., 2013 WL 2631062 (U.S. June 13, 2013) (naturally occurring DNA segment is a product of nature and not patent eligible merely because it has been isolated, but composite "cDNA" is patent eligible because it is not naturally occurring).

while assuming that those sections can do work that they are not equipped to do." The court also arguably further marginalized the "machine or transformation" test (which was originally limited in its *Bilski* opinion), intimating that a patent that satisfies the test could still be deemed unpatentable under §101: "[I]n stating that the 'machine-or-transformation' test is an 'important and useful clue' to patentability, we have neither said nor implied that the test trumps the 'law of nature' exclusion."

- **Nautilus, Inc v. Biosig Instruments, Inc.** – In this case, the Supreme Court rejected a standard to determine whether a patent claim was too indefinite, and therefore non-patentable.[212] The previous standard, which tolerated some ambiguous claims, but not others, stated that such patent claims can meet the Patent Act's definiteness requirement as long as such claims were "amenable to construction" and not "insolubly ambiguous."[213] standard on the grounds that it was insufficient to meet the standards of definiteness embodied in the Act The notion that a claim that is "amenable to construction" or not "insolubly ambiguous" could survive a definiteness challenge could "breed lower court confusion, for [these formulations] lack the precision the [Act] demands." To tolerate such a standard would "diminish the definiteness requirement's public-notice function and foster the innovation-discouraging 'zone of uncertainty.'" The court also noted that "it cannot be sufficient that a court can describe *some* meaning to a patent's claims; the definiteness inquiry trains on the understanding of a skilled artisan at the time of the patent application, not that of a court viewing matters *post hoc*."[214] Accordingly, the appropriate standard for ascertaining whether a claim is sufficiently definite depends on if those skilled in the art can be informed of the scope of the invention with reasonable certainty. Although the definiteness requirement must

212. 134 S. Ct. 2120 (2014).
213. Id. (citing Biosig Instruments, Inc. v. Nautilus, Inc., 715 F.3d 891 (Fed. Cir. 2013). This Supreme Court decision also abrogated a number of previous Federal Circuit cases on this topic. See, e.g., Hearing Components, Inc v. Shure Inc., 600 F.3d 1357 (Fed. Cir. 2010); Datamize, LLC v. Plumtree Software, Inc., 417 F.3d 1342 (Fed. Cir. 2005); Exxon Research and Engineering Co. v. U.S., 265 F.3d 1371 (Fed. Cir. 2001).
214. Biosig Instruments, Inc., 134 S. Ct. at 2130 (emphasis in original); see also Warner–Jenkinson Co. v. Hilton Davis Chemical Co., 520 U.S. 17 (1997) (if a test for definiteness cannot be at least "probative of the essential inquiry," it will fail).

take into account inherent limitations of language, the new standard mandates clarity when analyzing a patent claim.

Business method patents have produced much commentary in recent years. At one time, courts rejected a method of doing business as not being within the class of patentable subject matter. The Federal Circuit then ruled that patentability does not turn on whether the claimed subject matter does "business" instead of something else and thus business method inventions would be considered like any other process claims. In recent years, however, courts and the U.S. Patent and Trademark Office have seemingly become stricter with regard to their scrutiny of business method patents.

- **Alice Corp. Pty. Ltd. v. CLS Bank Intern.** – During the 2014 Term, the Supreme Court issued a ruling that centered on whether using a computer system to mitigate "settlement risk" was an abstract idea, and thus not patentable.[215] The Petitioner was an assignee of several patents that disclose a method of attenuating settlement risk, meaning that the patents were designed to facilitate the exchange of financial obligations between two parties via a computer system as a third-party intermediary.[216] In light of *Bilski*, the District Court held that all claims were ineligible for patent protection as recitations of an abstract idea, and the Federal Circuit affirmed. The high court agreed. First, the court determined that the patent claims at issue are directed to a patent-ineligible concept like laws of nature, natural phenomena, and abstract ideas. The Petitioner's claims were directed at abstract ideas, intermediated settlement, that like risk hedging, was deemed in *Bilski* to be a "fundamental economic practice long prevalent in our system of commerce." As such, the Petitioner's claims pertained to the abstract idea of intermediated settlement, and the court then turned to whether the method claims transformed the abstract idea into a patent-eligible invention.[217] Specifically, the

215. 134 S. Ct. 2347 (2014).
216. Id. at 2349. The patents at issue in the case claimed: (1) a method for exchanging financial obligations, (2) a computer system configured to carry out the method for exchanging obligations, and (3) a computer-readable medium containing program code for performing the method of exchanging obligations.
217. Alice Corp., 134 S. Ct., at 2355. The court cited to the framework established in Mayo Collaborative Services v. Prometheus Laboratories, Inc., 566 U.S. ____, 132 S. Ct. 1289 (2012). That test involves a two-step process for determining whether patent claims that refer to laws of nature, natural phenomena, or abstract ideas include patent-eligible applications of these concepts. First, the court must determine whether the claims at issue are directed to one of those patent-ineligible

method claims must contain an "inventive concept." The Supreme Court held that the Petitioner's method claims did not contain an "inventive concept" sufficient to render them patent-eligible. Rather, these claims merely instructed a "generic" computer to undertake functions, such as electronic recordkeeping, adjust account balances and obtain data that are "purely conventional," and "well-understood, routine, conventional activit[ies]."Accordingly, considering the claims as an "ordered combination" add nothing that is not already present when the steps are considered separately, and similarly does not improve the functioning of the computer itself.[218]

- **Ultramercial v. Hulu** – In 2014, in light of *Alice Corp.*, the Federal Circuit reversed its original decision in this case to hold that this method of contributing and monetizing copyrighted products via the Internet was no longer patent eligible under 35 U.S.C. § 101.[219] Given the "added benefit of the Supreme Court's reasoning in *Alice Corp.*," the court followed the framework established in the case to determine that "the concept embodied by the majority of the limitations describes [in the patent application] only the abstract idea of showing an advertisement before delivering free content."[220] As for

---

concepts. 132 S.Ct. at 1296-97. Second, the court will consider the elements of each claim both individually and as an "ordered combination" to determine whether "additional elements transform the nature of the claim" into a patent-eligible application. Id. at 1297, 1298.

218. see Mayo, 132 S. Ct. at 1294 (noting that transforming an abstract idea into a patent-eligible application requires more than "simply stat[ing] the [abstract idea] while adding the words 'apply it.'"); Parker v. Flook, 437 U.S. 584, 593 (1978) (observing that if a patent application could claim any principle of the sciences by reciting a computer system designed to implement the claim, such a result would make the determination of patent eligibility "depend on the draftsman's art).

219. 772 F.3d 709 (Fed. Cir. 2014). The overturned decision was Ultramercial, Inc. v. Hulu, Inc., 722 F.3d 1335 (Fed. Cir. 2013); but see Ancora Technologies, Inc., 744 F.3d 732 (Fed. Cir. 2014) (software method patent that prevented unauthorized software use by checking whether the software is operating within a license and stopping the program or taking other remedial action if it was not is patentable, and does not suffer from indefiniteness, as its use of the terms "volatile memory" and "nonvolatile memory" have a meaning that is "clear settled and objective in content").

220. 722 F.3d at 713. As discussed above, the test first espoused in *Alice Corp.* requires that a court confronted with patent applications (1) "determine whether the claims at issue are directed to one of those patent-ineligible concepts" and then (2) if the claims are found to be direct to one of the patent ineligible concepts, the court must thereafter determine "whether the claims contain an element or combination of elements that is sufficient to ensure that the patent in practice amounts to significantly more than a patent upon the [ineligible concept] itself."

the application of this abstract idea, the patent claims in question "simply instruct the practitioner to implement the abstract idea with routine, conventional activity." Of particular interest is that the Federal Circuit in the case reiterated the conclusion reached in *Bilski* that the "machine-or-transformation test is not the sole test governing § 101 analyses."

- **Bilski v. Kappos** – The machine-or-transformation test is not the sole test for patent eligibility under §101 because any ordinary, contemporary meaning of "process" under the Patent Act would not necessarily require it to be tied to a machine or the transformation of an article.[221] The Supreme Court affirmed the Federal Circuit's holding of unpatentability and found the patentee's claims, which sought to patent both the concept of hedging risk and the application of that concept to energy markets, were attempts to patent abstract ideas, not patentable processes. Most notably, the Court rejected the Federal Circuit's holding[222] that the "machine-or-transformation test" is the exclusive test for determining patentability of a process under §101, instead holding that the test remains a "useful and important clue," but not the "sole test" for determining whether an invention is a patent-eligible process under §101. The Court also refused to interpret the Patent Act to categorically exclude business methods.[223] The Court stated that the Act "leaves

---

Ultramercial, 772 F.3d at 715 (citing Alice Corp. Pty. Ltd. v. CLS Bank Intern., 134 S. Ct. 2347, 2355 (2014)) (internal quotations omitted).

221. Bilski v. Kappos, 130 S.Ct. 3218 (2010).
222. In Re Bilski, 545 F.3d. 943 (Fed. Cir. 2008). Regarding the Federal Circuit's *State Street* [State Street Bank & Trust Co. v. Signature Financial Group, Inc., 149 F. 3d 1368, 1373 (1998)] test, which the Federal Circuit repudiated in its *Bilski* opinion, the Supreme Court's majority opinion in *Bilski* neither explicitly endorsed nor rejected it, writing that "nothing in today's opinion should be read as endorsing interpretations of §101 that the Court of Appeals for the Federal Circuit has used in the past. See, e.g., State Street, 149 F. 3d, at 1373…." Bilski, 130 S.Ct. at 3231. However, the two concurring opinions (which were signed on by five Justices) explicitly rejected the *State Street* "useful, concrete and tangible result test." For example, Justice Stevens wrote that: "[I]t would be a grave mistake to assume that anything with a 'useful, concrete and tangible result,' may be patented." Id. at 3232, n. 1.
223. It should be noted that Justice Stevens's concurring opinion, which was joined by three other Justices, would have found methods of doing business to be unpatentable: "In the absence of any clear guidance from Congress, we have only limited textual, historical, and functional clues on which to rely. Those clues all point toward the same conclusion: that petitioners' claim is not a "process" within the meaning of §101 because methods of doing business are

open the possibility that there are at least some processes that can be fairly described as business methods that are within patentable subject matter under §101." The Court also noted that even if a particular business method fits into the statutory definition of a process, such a claim must still clear the statutory requirements for patentability, namely that any claimed invention be novel, non-obvious, and fully and particularly described. In closing, the Court reiterated its cautious approach to avoid imposing limitations on the Patent Act that are inconsistent with the text: "The patent application here can be rejected under our precedents on the unpatentability of abstract ideas. The Court, therefore, need not define further what constitutes a patentable "process," beyond pointing to the definition of that term provided in §100(b) and looking to the guideposts *Benson*, *Flook*, and *Diehr*."[224]

ELECTRONIC CONTRACTING

In today's technological world, any company may conduct some or all of its business electronically. Companies may enter into a contract via email or over the Internet, and just as messages sent using faxes, telex, telegraph, and other older communication methods can satisfy the Statute of Frauds, so too can emails exchanged between parties can form a valid contract. Companies and individuals may also contract by traditional or electronic means to license software, to buy or lease hardware, and/or to access or use a computer database. Whether the electronic element constitutes an incidental part of the subject matter of the contract, both traditional contract law concepts and issues specific to the electronic context may arise.

With the advent of mass-market software and Internet computer sales, individually negotiated contracts have largely been abandoned for practical reasons. On the Internet, Web pages or pre-installation screens often contain standardized clickwrap agreements, which are intended to take the place of any direct bargaining between the parties. These clickwrap agreements generally require online users to indicate their assent to the terms of an online agreement by means of conduct, such as by clicking

---

not, in themselves, covered by the statute. In my view, acknowledging as much would be a far more sensible and restrained way to resolve this case.".

224. See Gottschalk v. Benson, 409 U. S. 63 (1972); Parker v. Flook, 437 U. S. 584 (1978); Diamond v. Diehr, 450 U. S. 175 (1981).

on an "I agree" button before allowing users to access materials on the site or to install software.[225]

- **Nguyen v. Barnes & Noble Inc.** – A consumer brought a putative class action against a large retailer after his online order of a tablet computer at a discounted price during a liquidation period was cancelled.[226] The retailer then filed motion to compel arbitration of any claims arising from the putative class action based on a provision in its website Terms of Use mandating arbitration of any disputes arising from an alleged breach of such Terms. The Terms of Use, which were hyperlinked in the bottom left-hand corner of every page on the Barnes & Noble website alongside hyperlinked copyright notices and privacy policy. The plaintiff had not clicked on the "Terms of Use" hyperlink nor actually read the Terms of Use. Precedents required that since Nguyen had not read the Terms of Use, and therefore did not have actual knowledge of them, the validity of the agreement turns on whether the website puts a reasonably prudent user on inquiry notice of the terms of the contract.[227] Such inquiry notice depends on the design and content of the website and the agreement's webpage. Although the court conceded that Barnes & Noble had made its Terms of Use available via a conspicuous hyperlink on every page of the website, it ultimately refused to enforce the arbitration provision as the site otherwise provided no notice to users nor prompts them to any affirmative action to demonstrate assent.
- **Asch Webhosting Inc. v. Adelphia Business Solutions Investment LLC –** An ISP that terminated a service contract with a small downstream Internet access provider because of spam-related complaints may rely on an exculpatory clause to escape any liability

225. See, e.g., Swift v. Zynga Game Network, Inc., 805 F.Supp.2d 904 (N.D. Cal. 2011) (finding formation of a valid contract where the software in question involved a "modified clickwrap" process in which the terms of service were not visible on the page but were accessible via a hyperlink); Fteja v. Facebook, Inc., 841 F.Supp.2d 829 (S.D.N.Y. 2012) (same); Vernon v. Quest Comm's Int'l, Inc., 857 F.Supp.2d 1135 (D. Colo. 2012) (while the provider undoubtedly could have offered more "user friendly" access to the subscriber agreement, the facts demonstrate that plaintiffs had reasonable notice and access to the terms and conditions of the arbitration clause and agreed to the terms via a valid clickwrap agreement).
226. 763 F.3d 1171; see also 9 U.S.C. § 1 *et seq.* (requiring federal district courts to stay judicial proceedings and compel arbitration claims covered by a written and enforcable arbitration agreement).
227. Nguyen, 763 F.3d at 1177 (citing Specht v. Netscape Communications Corp., 306 F.3d 17 (2d Cir. 2002)).

because such a limitation of liability is not unconscionable or against New Jersey public policy.[228] The appeals court affirmed the dismissal of the plaintiff's breach of contract action. The court stated that enforcing an exculpatory clause after an alleged willful breach of contract does not necessarily violate public policy, particularly since there was no evidence of unequal bargaining power between the parties when the plaintiff was a commercial entity managed by an experienced businessman well-versed with ISP agreements. The court also found that given that the defendant ISP gave the plaintiff notice and the opportunity to find another provider before terminating its service, enforcing the exculpatory clause under such circumstances was not oppressive or unreasonable.

- **Surplus.com, Inc. v. Oracle Corp.** – A software development agreement that included provisions for maintenance and technical support did not render the software a "service" instead of a "good" such that the agreement is governed under UCC Article 2.[229] The court granted the defendant's motion to dismiss, finding that the four-year statute of limitations for breach of contract under the UCC applied to the plaintiff's claims. The court found that although the custom software development entailed the provision of services–even software development services that were performed by an outside entity–those services were ancillary to the software that was the heart of the relevant agreement. The court concluded that the agreement's provision for maintenance and technical support did not render the software a "service" rather than a "good" under the UCC.
- **In re Zappos.com, Inc.** – An arbitration clause contained in a browsewrap agreement that could be accessed via an inconspicuous

228. Asch Webhosting Inc. v. Adelphia Business Solutions Investment LLC, 2010 WL 258784 (3d Cir. Jan. 25, 2010) (non-precedential). See also Duffy v. The Ticketreserve Inc., 2010 WL 2681045 (N.D. Ill. July 6, 2010) (most contract claims against an online sporting ticket options marketplace based upon fraudulent third-party tickets were dismissed, with leave to amend; the court enforced the limitations of liability and broad release in the online user agreement); but see Rottner v. AVG Technologies, 2013 WL 1857076 (D. Mass. May 3, 2013) (disclaimers contained in EULA for downloadable software may effectively disclaim implied warranties, as permitted under UCC Article 2, but cannot disclaim express warranty claims based upon statements made in advertising copy touting the software's functionality).

229. Surplus.com, Inc. v. Oracle Corp., 2010 WL 5419075 (N.D. Ill. Dec. 23, 2010). But see Digital Ally, Inc. v. Z3 Technology, LLC, 2010 WL 3974674 (D. Kan. Sept. 30, 2010) (software license agreement does not involve transfer of title and so was not a sale of goods for UCC Article 2 purposes under Nebraska law).

link buried in the middle to bottom of every webpage, among many other similarly-looking links where no reasonable user would have reason to click, was unenforceable.[230] The court denied the defendant's motion to compel arbitration of a data security-related dispute because the terms of use were not enforceable. The court found that the e-commerce site did not direct users to the browse-wrap terms of use when users created an account, logged into an existing account, or made a purchase. As the court noted, "a party cannot assent to terms of which it has no knowledge or constructive notice, and a highly inconspicuous hyper link buried among a sea of links does not provide such notice." Alternatively, the court stated that the arbitration agreement was otherwise an unenforceable, illusory contract because the terms of use contained language that granted the site the unilateral, unrestricted right to revise the terms without notice.

- **Defontes v. Dell** – An arbitration clause in a computer purchase shrinkwrap license was deemed unenforceable where the language of the terms and conditions agreement included with the goods did not reasonably inform the consumer class that they could reject the terms simply by returning the goods.[231] The Rhode Island Supreme

230. In re Zappos.com, Inc., 2012 WL 4466660 (D. Nev. Sept. 27, 2012). See also Knutson v. Sirius XM Radio, 771 F.3d (9th Cir. 2014) (arbitration provision in browsewrap agreement nonbinding since a reasonable person would not believe that purchasing a vehicle from Toyota would also bind him to any contract with Sirius XM, particularly because the Sirius XM service was believed to be complimentary and the purchaser never received any documents from Sirius XM); Schnabel v. Trilegiant Corp., 2012 WL 3871366 (2d Cir. Sept. 7, 2012) (email sent after user signed up for third-party marketing program following an online purchase did not provide sufficient notice to the plaintiffs of an arbitration provision, and the plaintiffs could not have assented to it solely as a result of their failure to cancel their enrollment in the defendants' service); but see Hancock v. AT&T, Inc., 2012 WL 6132070 (10th Cir. Dec. 11, 2012) (communications company practice of presenting terms for TV/voice service via a clickwrap agreement on its technician's laptop during the installation process and thereafter offering a separate clickwrap agreement presented on users' computers for internet services is enforceable and offers users an adequate opportunity to manifest assent to the terms; court enforced forum selection and arbitration clauses in those agreements, finding no decision which prohibits a provider from offering separate electronic agreements for different services); Swift v. Zynga Game Network, 805 F. Supp. 2d 904 (N.D. Cal. 2011) (finding formation of a valid contract where the software in question involved a "modified clickwrap" process in which the terms of service were not visible on the page but were accessible via a hyperlink).

231. Defontes v. Dell, 984 A.2d 1061 (R.I. 2009).

court upheld the lower court's ruling declaring the arbitration clause unenforceable. The court found that the terms and conditions of the shrinkwrap license required "too many inferential steps" of the plaintiffs and "too many of the relevant provisions were left ambiguous," such that a reasonably prudent offeree would understand that by keeping the purchased computer he or she was agreeing to be bound by the terms and conditions agreement and retained, for a specified time, the power to reject the terms by returning the product.

- **AT&T Mobility LLC v. Concepcion** – Because it stands as an obstacle to placing arbitration agreements on an equal footing with other contracts, California's *Discover Bank* rule – which held that class action waivers in consumer arbitration agreements were unconscionable if the agreement was in an adhesion contract, disputes between the parties were likely to involve small amounts of damages, and the party with inferior bargaining power alleged a deliberate scheme to defraud – is preempted by the Federal Arbitration Act.[232]
- **Anderson v. Bell** – A candidate may use electronic signatures to satisfy the signature requirement that Utah law imposes on those unaffiliated with a political party who wish to run for statewide office.[233] The state supreme court granted the plaintiff's petition to compel state election officials to count the electronic signatures submitted in support of his candidacy for governor. The court found that while the legislature designed the Election Code with a paper format in mind, the legislature also left open the possibility that a signor may lend his name to a certificate for nomination in electronic ways when it passed the Uniform Electronic Transactions Act (UETA), which "applies to electronic records and electronic signatures relating to a transaction." The court found that UETA's list of exceptions was silent on the topic of elections and campaigning. The court also rejected the state agency's argument that as a party

232. AT&T Mobility LLC v. Concepcion, 131 S.Ct. 1740 (2011). See also Coneff v. AT&T, 2012 WL 887598 (9th Cir. Mar. 16, 2012) (a narrow, fact-based state-law rule for voiding class action waivers under Washington law does not fall outside of *Concepcion*; the FAA preempts the Washington state law invalidating the class-action waiver).

233. Anderson v. Bell, 2010 WL 2485545 (Utah June 22, 2010). See also Rosas v. Macy's Inc., 2012 WL 3656274 (C.D. Cal. Aug. 24, 2012) (employee's electronic signatures on acknowledgment forms formed valid and enforceable agreement to arbitrate; employee admitted receiving employee handbook and signing the Acknowledgment Form, such that his failure to opt out of company arbitration program within set time period constituted assent to the arbitration agreement).

to the transaction, it must agree to conduct the transaction by electronic means before the electronic signature is valid. The court found that while UETA permits governmental agencies to dictate what transactions they are willing to conduct through electronic means and what transactions they are unwilling to do via electronic means, the statute contemplated that the state first enact such restrictions via rulemaking, something the state had not done in this case.

JURISDICTION AND PROCEDURE

As plaintiffs increasingly have urged courts to exercise jurisdiction over non-resident parties based on their Web presence, two lines of analysis have arisen in the judicial opinions. One line of reasoning developed from the opinion in *Zippo Manufacturing Co. v. Zippo Dot Com Inc.*,[234] where the court proposed that "the likelihood that personal jurisdiction can be constitutionally exercised is directly proportional to the nature and quality of commercial activity that an entity conducts over the Internet." The *Zippo* court established a "sliding scale" of Internet activity. On one end of the scale lie passive sites that only provide information and do not allow any interaction between a user and the website, and thus, are unlikely to provide a basis for the exercise of jurisdiction. On the other end of the scale are fully interactive websites where a defendant conducts business over the Internet, a site much more likely to provide a basis for the exercise of jurisdiction.

Another line of cases follow the reasoning of the Supreme Court's decision in *Calder v. Jones,*[235] a pre-Internet defamation case in which the Court held that jurisdiction could be premised on the intentional conduct of defendants outside the forum state that is calculated to cause injury to the plaintiffs within the forum state. Courts typically apply the *Calder* "effects test" in cases involving defamation or some other intentional tort, including trademark infringement.

- **Guffey v. Ostonakulov** – In 2014, the Oklahoma Supreme Court held that a Tennessee-based used car dealer that used eBay to sell a

234. 952 F.Supp. 1119 (E.D. Pa. 1997).

235. 465 U.S. 783, 104 S.Ct. 1482, 79 L.Ed.2d 804 (1984); but see Trachtenberg v. Failedmessiah.com, –- F. Supp. 2d —, 2014 WL 4286154 (E.D.N.Y. Aug. 29, 2014) (noting that the New York long-arm statute is narrower than the federal standard in refusing personal jurisdiction in a defamation case since the defendant did not develop any content while physically present in New York) .

car to an Oklahoma resident could be subjected to jurisdiction in Oklahoma.[236] It reasoned as such because the defendant utilized eBay for regular business within the jurisdiction, he had exchanged emails with the plaintiff outside of the auction, and the sale created an ongoing obligation in Oklahoma in the form of a warranty. However, at least one circuit has held that the sale of an automobile via eBay is not in and of itself sufficient to establish minimum contacts.[237]

- **Zynga Game Network Inc. v. Does** – An online videogame company that sought discovery from third-party web hosting companies and other websites seeking the identity of domain name holders who are allegedly operating infringing websites must narrow the scope of its subpoenas to information related to the identify and name the John Doe defendants.[238] The court granted the plaintiff's motion to conduct limited discovery, but narrowed the scope of the subpoenas, stating that the plaintiff's request for items such as server logs, website content transaction histories and correspondence remotely linked to the defendants was overbroad. The court ultimately limited the reach of the subpoena to "all documents necessary to obtain the name, current and permanent addresses, telephone numbers, and valid email addresses of the owner(s) of [the defendant's allegedly infringing website] or similar information suitable for identification and location of defendants."
- **Penguin Group (USA) Inc. v. American Buddha –** In copyright infringement cases involving the uploading of a copyrighted printed literary work onto the Internet, the situs of injury for purposes of determining long-arm jurisdiction under C.P.L.R. § 302(a)(3)(ii) is the location of the principal place of business of the copyright

236. 321 P.3d 971 (Okla. 2014).
237. See Borchetto v. Hansing, 559 F.3d 1011 (9th Cir. 2008).
238. Zynga Game Network Inc. v. Does 1-5, 2010 WL 271426 (N.D. Cal., Jan. 21, 2010). See also Pacific Century Int'l Ltd. v. Does, 2011 WL 2690142 (N.D. Cal. July 8, 2011) (mere allegation that multiple Doe defendants used the same BitTorrent network to infringe a copyrighted work is insufficient to meet the standards for joinder set forth in Rule 20; court found no evidence that users acted together to download the work, despite the collaborative nature of members of a BitTorrent "swarm"); R&D Film 1 LLC v. Does 1-103, No. 12 - 09041 (N.D. Ill. Jan. 8, 2013) (finding joinder inappropriate based solely on defendants' participation in the same BitTorrent swarm); Malibu Media LLC v. John Doe No. 4, 2012 WL 5987854 (S.D.N.Y. Nov. 30, 2012) (defendant's motion to quash subpoena to ISP denied, but court permitted the defendant to remain anonymous on account of privacy-related concerns).

holder.[239] In answering a certified question from the Second Circuit, the New York Court of Appeals rejected the defendant's argument that a derivative economic injury felt in New York based solely on the domicile of the plaintiff was insufficient to establish an in-state injury within the meaning of the long-arm statute. The court commented that in the case of online infringement and digital piracy, where the harm is dispersed throughout the country, the place of uploading is inconsequential and it is difficult, if not impossible, to correlate lost sales to a particular geographic area, such that the out-of-state location of the infringing conduct carries less weight in the jurisdictional inquiry. Indeed**,** the court noted: "the absence of any evidence of the actual downloading of Penguin's four works by users in New York is not fatal to a finding that the alleged injury occurred in New York."

- **Internet Solutions Corp. v. Marshall –** A nonresident defendant commits the tortious act of defamation in Florida for purposes of Florida's long-arm statute when the nonresident makes allegedly defamatory statements about a Florida resident by posting those statements on a website, provided that the website posts containing the statements are accessible in the forum and accessed in the forum.[240]

---

239. Penguin Group (USA) Inc. v. American Buddha, 2011 NY Slip Op 02079 (N.Y. Mar. 24, 2011). Following the ruling by the New York Court of Appeal on the certified question, the Second Circuit vacated the lower court's order and remanded to determine whether the plaintiff established the four remaining jurisdictional requisites under the New York long-arm statute, and the extent to which the assertion of personal jurisdiction would be consistent with the requirements of Due Process. Penguin Group (USA) Inc. v. American Buddha, 640 F.3d 497 (2d Cir. May 12, 2011). On remand, the district court dismissed the action for lack of jurisdiction because the plaintiff failed to show that the defendant derived "substantial revenue from interstate or international commerce" as required under the long arm statute. See Penguin Group (USA) Inc. v. American Buddha, 2013 WL 865486 (S.D.N.Y. Mar. 7, 2013). See also MacDermid, Inc. v. Deiter, 2012 WL 6684580 (2d Cir. Dec. 26, 2012) (Connecticut court may properly exercise long-arm jurisdiction over a defendant who, while domiciled and working in Canada, allegedly accessed a computer server located in the forum to misappropriate confidential information belonging to her employer). But see Troma Entertainment Inc. v. Centennial Pictures Inc., 2012 WL 1178998 (E.D.N.Y. Apr. 9, 2012) (mere claims of infringement against New York copyright holder is insufficient to trigger *Penguin* rule; downloading of films over the Internet and subsequent unauthorized licensing of the works is far different than the uploading of copyrighted works and online distribution that occurred in *Penguin*).

240. Internet Solutions Corp. v. Marshall, 2010 WL 2400390 (Fla. June 17, 2010). But see Penachio v. Benedict, 2012 WL 10971 (2d Cir. Jan. 4, 2012) (out-of-state witnesses in a family court proceeding who posted allegedly defamatory

In answering this certified question from the Eleventh Circuit, the Florida Supreme Court did not address the second part of the long-arm jurisdictional analysis, namely whether an exercise of jurisdiction over a non-resident defendant under these circumstances violates the due process clause.

- **Consulting Engineers Corp. v. Geometric Ltd. –** Foreign software developers were not subject to personal jurisdiction in a Virginia forum based upon email and telephone contacts concerning a project in India, particularly since no agreement to perform work was ever reached.[241]

videos on YouTube, but had no related commercial interest in the forum, are not amenable to long-arm jurisdiction in New York).

241. Consulting Engineers Corp. v. Geometric Ltd., 561 F.3d 273 (4th Cir. Mar. 23, 2009). But see Gallup, Inc. v. Business Research Bureau (PVT.) Ltd., 2008 WL 4857027 (N.D. Cal. Nov. 10, 2008) (federal court had subject matter jurisdiction over foreign defendants to hear the plaintiff's Lanham Act claims based upon allegation that "Gallup" trademark had an adverse effect on U.S. commerce).

NOTES