Chapter 12

INTERNET PUBLISHING

By Mark Sableman and Jennifer A. Visintine
Thompson Coburn, LLP
St. Louis, Missouri

The law of Internet publishing is just like normal publishing law … with a few special twists. Congress and the courts have tailored some special legal doctrines to cover certain aspects of Internet publishing. News media companies that make use of the Internet need to understand and utilize these special rules.

Background: Traditional Media Liability for User Content and Actions

Many media companies permit subscribers and members of the general public to post content to their websites. Such postings take many forms: message boards, comments in forums, reader comments to articles, guest bloggers, etc. In one sense, such content is simply an electronic version of the time-honored "letters to the editor" section of a newspaper. But there are both practical and legal distinctions. As a practical matter, because of the volume and timing of Internet postings, and because postings can be accomplished with no editorial intervention, news organizations usually allow the postings with no prior editorial review, or a much less rigorous editorial review than for letters to the editor.

As a result, there is a significant risk that inappropriate, defamatory, or otherwise harmful or unlawful content may find its way to the public forum portions of media websites. Unedited user content on media websites thus raises the question: To what extent is the media organization (or any web publisher, for that matter) liable for user-generated content? The answer is that Congress has exempted web publishers from certain liabilities that would accompany similar activities in print.

Under traditional publishing law principles, a publisher or broadcaster is potentially liable for all content it publishes. Generally, "one who repeats or otherwise republishes defamatory matter is subject to liability as if he had originally published it.[1] Thus, under traditional law, even an innocent publisher or distributor of third-party content could be held liable for defamation and other content-based tort claims.

These traditional principles proved to be problematic in the Internet era. Accordingly, Congress enacted two special laws that create special liability exemptions for Internet intermediaries such as Internet service providers ("ISPs") and website operators—including media companies. These rules are contained in two landmark pieces of legislation: the Telecommunications Act of 1996 and the Digital Millenium Communications Act ("DMCA"). All persons who act as Internet intermediaries, including traditional media companies that maintain an online presence, need to understand these laws, described in Sections I and II below.

Media companies may also receive subpoenas seeking information about those who post comments or materials on their websites. Both statutes and a developing body of court decisions in this area, described in Section III below, govern such subpoenas.

.

I. LIABILITY FOR USER-GENERATED CONTENT ON THE INTERNET

A. Prior Law; Need for Legislation

Prior to the Telecommunications Act of 1996, Internet intermediaries faced potential liability for all of the postings that they carried or transmitted.

In a leading case arising out of the early days of online activity, *Cubby v. CompuServe, Inc*.,[2] a court held that an online distributor could be held liable for the content it made available online. In that case, Cubby, an allegedly defamed party, claimed that the CompuServe online service was liable for a statement about him on one of its content services. The actual publication that created and carried the statement about Cubby was "Rumorville USA," a news service carried on CompuServe's "Journalism Forum." CompuServe argued that it should not be liable for the publication because it was a mere distributor of third-party content—akin to a newsstand or a bookstore—rather than a publisher of the defamatory statements. The court accepted that publisher/distributor distinction, but went on to find that even mere distributors, like

CompuServe, can be liable for libel once they know or have reason to know of the defamatory publication. The result was that whenever anyone complained to an online distributor (such as an ISP or a website operator), that distributor was potentially liable—and then faced with the unenviable choice of either taking down the posting or having to defend the publication.

In a key follow-up case to *Cubby*, *Stratton Oakmont, Inc. v. Prodigy Servs. Co*.,[3] the plaintiff sued another online service provider, Prodigy, claiming to have been defamed by third-party content posted on Prodigy. Prodigy argued that, like CompuServe in the *Cubby* case, it was an innocent disseminator of the information, and should at least receive the benefit of the defense available to distributors with no knowledge of the defamatory material. In *Stratton Oakmont*, however, the court held that because Prodigy engaged in editorial activities, screening some offensive material from its subscribers, Prodigy fell into the position of a "publisher" rather than a "distributor," and could not avail itself even of the limited distributor defense recognized in the *Cubby* case. Essentially, *Stratton Oakmont* held that an online provider that attempted to conduct any editorial control over its service, even including just screening for objectionable words, would be saddled with full traditional publisher liabilities.

As a consequence of the *Cubby* and *Stratton Oakmont* cases, the ISP community became seriously concerned about the risks that ISPs would face for merely hosting and re-transmitting their subscribers' content. Accordingly, the Internet industry complained to Congress that the *Cubby* and *Stratton Oakmont* decisions could cripple the online provider industry, since no one would willingly retransmit large amounts of third-party content (as online providers must do) if they face potentially unlimited liability for that content. As a result, Congress subsequently enacted Section 230 of the Telecommunications Act of 1996 ("section 230"; sometimes referred to by the title of the chapter in which it was contained, the Communications Decency Act).

B. Section 230: Immunity for Internet Intermediaries

Section 230 made it possible for ISPs and website operators (including media companies) to accept, post, and transmit messages of users without facing potential liability under *Cubby* and *Stratton Oakmont*.

Initially, section 230 created a special statutory exemption from the standard rules of *Stratton Oakmont* and *Cubby*, by exempting Internet intermediaries from the content-based liabilities of third parties:

> No provider or user of an interactive computer service shall be treated as a publisher or speaker of any information provided by another information content provider.[4]

It also imposed in its "Good Samaritan" provision a complete immunity to Internet intermediaries that impose any kind of screening or editorial control over third-party content:

> No provider or user of an interactive computer service shall be held liable on account of -
>
> (A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected[.][5]

In short, section 230 provides immunity for ISPs for causes of action that arise out of Internet content which was posted by any third party. It is a broad immunity, in who and what it covers.

Who is covered. Section 230 covers all providers and users of "interactive computer services." This definitely covers ISPs—companies that make Internet access available to customers. But it also covers anyone who operates a website, and it even includes people who *use* the Internet (*i.e.*, a "user" of "interactive computer services").

Most importantly, section 230 grants these persons immunity so long as they are not the author (or co-author) of the content in question. That is, where information is provided by a third party ("another information content provider"), a website operator (such as a newspaper or television station that operates a website) shall *not* be treated as the "publisher or speaker" of that information. That in turn means (at least under the prevailing interpretation, in the *Zeran* case explained below) that the service provider will not be liable for the third party's content.

What it covers. Section 230 protects covered persons from any content-based tort liabilities, including traditional publishing-based liabilities such as libel and invasion of privacy. It has been interpreted to provide immunity for a wide variety of claims, including causes of action alleging libel, invasion of privacy, negligence, breach of contract, fraud, negligent infliction of emotional distress, negligent misrepresentation, breach of warranty, right of publicity, and violations of the Fair Housing Act and other laws prohibiting discrimination.[6] The Good Samaritan provision has also immunized ISPs facing claims alleging a violation of First Amendment free speech rights.[7] Section 230 does not, however, cover criminal charges or claims arising under intellectual property laws.

W**hat kind of editorial contributions are allowed.** In *Stratton Oakmont*, it should be remembered, the defendant, Prodigy, was found to be a "publisher" with a high level of potential liability, simply because it had performed some editorial screening functions for its online service. In section 230, Congress assured Internet operators that doing what Prodigy did —or indeed taking *any* kind of preventative screening or after-the-fact editorial actions—were fully permitted and encouraged, and would not subject the operator to further liability. In its "Good Samaritan" provision, section 230 specifically exempts intermediaries from any liability based upon their screening of material posted on their websites.[8]

Thus, because of the Good Samaritan provision, and because section 230 immunity extends only to intermediaries that post comments *of third parties,* even where a news website specifically reviews and selects the messages that it permits on its website, thereby exercising what would normally be considered significant editorial discretion, that activity would not affect the section 230 immunity. Most courts hold that when traditional editorial functions of a publisher are involved, the defendant will not be found to have crossed the line into joint authorship. The prevailing exemption for normal editing activity was acknowledged in a leading case, *Barrett v. Rosenthal*, where the California Supreme Court noted that "active involvement in the creation of a defamatory Internet posting" does not get the benefit of the §230 immunity.9

What constitutes authorship or co-authorship. Not everything that a service provider does constitutes a mere transmittal, or editing, of third party content. Service providers also engage in authorship of their own, and automated processes can cause such authorship to arise in unexpected places. In one important ruling, the Ninth Circuit federal court of appeals, in *Fair Housing Council of San Fernando Valley v. Roommates.com,*[10] found a website operator liable when it essentially directed its users to make choices which would violate federal housing law. Where, for example, federal housing law prohibited discrimination on the basis of certain classifications, the website nonetheless required its users to advertise for housing using those legally forbidden classifications. In these circumstances, the court found that the website operator was not a true intermediary for the content of third parties. Rather, it had so directed its user's choices that it was effectively the author or co-author of the content.

Judicial interpretations. Most courts have broadly interpreted the language of Section 230.[11] The leading case is *Zeran v. America Online, Inc*.[12] In that case, the plaintiff Zeran alleged that America Online ("AOL") was liable for defamatory statements posted by a third party on AOL's bulletin boards because, among other things, AOL unreasonably delayed in removing such statements from its bulletin boards and failed to screen for similar postings after it had been notified of their false and defamatory nature. In reaching its decision, the *Zeran* court considered the purpose of section 230 and the circumstances surrounding Congress' adoption of section 230, noting that its purpose is "to maintain the robust nature of Internet communication and accordingly, to keep governmental interference in the medium to a minimum." Thus, the court ultimately affirmed the district court's grant of summary judgment in favor of AOL, finding that it was not liable for defamation even though it was aware of the allegedly defamatory statements. In effect, the *Zeran* court determined that section 230 not only immunizes ISPs from claims where they are treated as a publisher, but also immunizes ISPs from *distributor* liability claims such as those at issue in *Cubby*.[13]

A few courts have taken a narrower view of Section 230, suggesting that it was meant only to provide Good Samaritan protection (that is, that it was meant to overrule *Stratton Oakmont*), but not to exempt distributors from their ordinary content-based liabilities (that is, it was *not* meant to overrule *Cubby*).[14]

Exemptions. Section 230 shall not "be construed to limit or expand any law pertaining to intellectual property."[15] Thus, it does not immunize ISPs for trademark infringement.[16] For example, in *Gucci America, Inc. v. Hall & Assocs.*,[17] Gucci filed an action against Mindspring, the host of a website that sold goods that infringed Gucci's trademarks. Gucci had twice notified Mindspring of the infringement, but Mindspring did not take action against the operator of the website. Mindspring moved to dismiss Gucci's claims on the grounds that section 230 immunized it from liability for information posted on the infringing website. The court rejected this claim, however, noting section 230's intellectual property exemption. The court stated that publishers may, under certain circumstances, be held liable for infringement under existing intellectual property laws, and that a distributor may be liable for infringement if it "continues to supply its product to one whom it knows or has reason to know is engaging in trademark infringement."[18]

Copyright infringement liabilities of ISPs are also not affected by section 230, because of the intellectual property exemption. Rather, they are governed by the Digital Millenium Copyright Act, discussed below.

State law claims relating to trade secrets and the right of publicity fall into a gray area; it is not clear whether they will be considered "intellectual property" exempt from section 230. Some courts have applied the "intellectual property" exception only to *federal* intellectual property claims, thereby providing ISPs with immunity for intellectual property claims arising under state law.[19] Other courts, however, have indicated (or assumed) that the intellectual property exception applies to both federal and state intellectual property laws, and that ISPs may thus be liable for state law causes of action, like right of publicity claims, that are closely akin to traditional intellectual property.[20]

II. CONTRIBUTORY LIABILITY FOR USER COPYRIGHT INFRINGEMENT ON THE INTERNET

A. Prior Law

Just as with content-based claims, under pre-Internet law, Internet intermediaries faced potential copyright liability for facilitating their customers' unlawful actions. Especially in our multi-media world, with increasing use of "citizen journalism" (photographs and videos submitted to news websites by readers), news websites face potential copyright liabilities.

In a leading case arising in the early days of popular Internet use, *Religious Technology Center v. Netcom, Inc*., an Internet service provider, Netcom, was held potentially liable for copyright infringement when a customer had used Netcom's service to transmit and post documents that infringed a copyright owner's rights. Specifically, *Netcom* held that an ISP could be held liable for contributory infringement if the ISP, "with knowledge of the infringing activity, induces, causes or materially contributes to the infringing conduct of another."[21] Additionally, an ISP with knowledge that its subscriber's activities infringed another's copyright could be liable for contributory infringement if it did not prevent further distribution of the infringing materials.[22]

While the decision recognized some limits on Netcom's potential "contributory infringement" liability—for example, it held that Netcom would not be liable unless it continued to permit the infringement to occur after the copyright owner notified it of the infringement—the Internet service provider industry found the ruling chilling. In effect, it required service providers to either closely police their customers' actions or cut off their customers once a copyright owner complained of possible infringement. Either option seemed to inhibit the growth of Internet use and the Internet industry.

B. The DMCA: A Balance Struck Between Service Providers and Copyright Owners

In response to the dual concerns of service providers (concerned about potential liabilities under the *Netcom* ruling) and copyright owners (concerned about the need to protect their works from easy infringement on the Internet), Congress passed the online liability limitation provisions of the Digital Millenium Copyright Act ("DMCA") in 1998. These provisions limit contributory and vicarious liability for copyright infringement claims.[23]

The DMCA attempts to strike a balance between the rights and responsibilities of ISPs and copyright owners. Essentially, ISPs who seek its protection (by registering with the Copyright Office) are given a "safe harbor" from copyright liability (*i.e.*, the liability they would have had under *Netcom*), so long as they follow a regimented notice-and-takedown procedure. That notice-and-takedown procedure protects copyright owners by giving them a simple way to get infringing works taken down, and of identifying apparent infringers.

Safe Harbors. The DMCA technically contains four safe harbors, which limit service provider liability for (1) acting as a conduit for the transmission of information by others;[24] (2) system caching;[25] (3) infringing materials residing on the ISP's system at the direction of the user;[26] and (4) linking users to online locations containing infringing materials.[27] The most important safe harbor is the one that exempts service providers from liability for material that resides on the ISP's network at the direction of its customers or users. Under this safe harbor, the ISP must:

1. have designated an agent to receive notifications of alleged infringement;[28]

2. not have actual knowledge that material posted on the Internet is infringing or be aware of facts or circumstances suggesting infringing activity, or upon obtaining such knowledge, act expeditiously to remove, or disable access to, the material;[29]

3. not receive any financial benefit "directly attributable" to the infringing activity;[30] and

4. upon notification of claimed infringement, respond expeditiously to remove or disable access to the allegedly infringing material.[31]

Of course, each of these requirements (as well as the requirements for the other limitations on liability) has been subject to litigation over the meaning of its particular terms.

While compliance with the safe harbor requirements does not render the service provider immune from copyright infringement claims, it does protect most providers from all monetary and most equitable relief.[32]

Notice-and-Takedown Procedures. A notice-and-takedown procedure makes up the heart of the DMCA's online liability provisions. When a copyright owner becomes aware that its copyrighted work has been posted on the Internet without its authorization, it may notify the ISP of the alleged infringement. An effective notification must comply with the terms of the statute.33 It must be a written communication provided to the service provider's designated agent, and must contain certain information, including a description of the allegedly infringed work and the infringing material, and information that will permit the service provider to locate the infringing material.[34] Upon receiving such notification, the ISP must follow the terms of the DMCA in order to preserve its immunity. It must either remove the allegedly infringing material from a website, or disable access to the material (and such disabling must meet certain requirements).[35] The ISP must also notify its subscriber that it has removed or disabled access to the material.[36] In response, the subscriber may submit a "counter

notice," which must include a description of the material that has been removed or to which access has been disabled, the location of the material before it was removed, and a statement that the subscriber has a good faith belief that the material was removed or disabled as a result of a mistake or misidentification of the material.[37] If the ISP receives such a "counter notice," the ISP must provide a copy of it to the copyright owner, and must inform that person that it will replace the removed material or cease disabling access to it in 10 days.[38] Finally, the ISP must replace the material or cease disabling access to it within 10-14, business days following receipt of the counter notice, unless the copyright owner informs the ISP's registered agent that it has filed an action seeking a court order to restrain the subscriber from engaging in the allegedly infringing activity.[39] The DMCA contains a subpoena provision allowing copyright owners to expeditiously determine the identity of posters of infringing materials.

In essence, the notice and takedown procedure allows copyright owners to have infringing material removed, or to have the opportunity to bring an infringement claim in court against the original poster. It also allows ISPs to escape intermediary liability, so long as they cooperate as notice-and-takedown traffic cops.

Protections against overbroad claims. The DMCA also contains provisions that seek to protect persons who post materials who are falsely charged with infringing copyrighted works. Copyright owners are directed not to assert DMCA claims beyond the scope of their legitimate copyright interests, as the statute specifically penalizes such overbroad claims.[40] Specifically, the DMCA provides that any person who "knowingly materially misrepresents … that material or activity is infringing … shall be liable for any damages, including costs and attorneys' fees, incurred by the alleged infringer."[41] Thus, any person who sends a DMCA violation notice with knowledge that its infringement claims are false may be liable for damages.[42] This can apply even where the copyright owner's content has clearly been copied.

The Northern District of California addressed this issue in *Lenz v. Universal Music Corp.*[43] In that case, the plaintiff, Ms. Lenz, posted a 29-second video of her children dancing to the song "Let's Go Crazy," by Prince, on YouTube.com. Universal sent a DMCA take-down notice to YouTube, demanding that it remove the video from the Internet. YouTube did so, and notified Ms. Lenz, who then asserted that her video constituted fair use of "Let's Go Crazy" and did not infringe Universal's copyrights. She demanded that the video be re-posted, and filed suit against Universal, alleging that it acted in bad faith when it issued its notice and take-down letter, and thus made a misrepresentation in violation of the DMCA. Universal argued that "copyright owners cannot be required to evaluate the question of fair use prior to sending a takedown notice because fair use is merely an *excused* infringement of a copyright rather than a use *authorized* by the copyright owner or by law." The court, however, rejected this argument, and found that Universal's takedown notice was overbroad and improper.

Additional requirements for ISPs. While most ISPs and other Internet intermediaries focus their attention almost exclusively on compliance with the DMCA's notice-and-takedown requirements, many copyright owners contend that the DMCA requires intermediaries to actively police their services to some extent. For example, the DMCA requires ISPs to implement policies that terminate repeat infringers.[44] Under general liability principles, moreover, intermediaries could be liable for providing a platform for infringers with the object and intent of promoting infringement.[45] Some media organizations have established and decided to follow a set of guidelines for user-generated content, which were designed to ensure adequate (or some might say, more than adequate) preventative measures against infringement.[46] The DMCA also requires ISPs accommodate and not interfere with standard technical measures used by copyright owners to identify or protect copyrighted works.[47]

III. DISCOVERY RELATING TO ANONYMOUS POSTINGS ON MEDIA WEBSITES

Where media websites contain anonymous or pseudonymous postings, persons aggrieved by the postings may seek the original poster's identity, either informally or though judicial processes. Such inquiries raise legal concerns.

A. Informal Requests

Where the poster is a subscriber to an electronic communications service (as, for example, a customer of an ISP), the provider may be limited in its ability to disclose the poster's identity in the absence of formal legal process. Specifically, the Electronic Communications Privacy Act ("ECPA")[48] imposes strict requirements on providers of electronic communication services and remote computing services with respect to what information they can give up about subscribers, even in response to lawful subpoenas and other legal requests. Where a media entity's online activities include not only publication of an online newspaper but also the provision of Internet services or remote computing services to subscribers, the operator might qualify as an electronic communications service provider or a remote computing service provider under the ECPA, and thus would be subject to its stringent subscriber privacy provisions. For example, in one case, America Online, in its capacity as a provider of Internet access services, released information to a governmental official about a subscriber in violation of the ECPA, and the subscriber brought various claims against AOL and others involved in the disclosure.[49]

B. Subpoenas for an Anonymous Poster's Identity

Often parties aggrieved by anonymous postings seek to obtain the poster's identity by (a) filing a lawsuit against the poster, naming him or her as a "John Doe" or "Jane Doe," and (b) immediately using that lawsuit to subpoena the website host or other party that may have knowledge of the poster's identity (or information that could lead to determining his or her identity). In some cases, courts may grant such subpoenas without considering their implications. These subpoenas raise First Amendment concerns, because the United States Supreme Court has recognized a right to speak with anonymity, and has acknowledged that "the freedom to publish anonymously extends beyond the literary realm."5[0]

Where subpoenas seeking the identity of anonymous posters have been litigated, courts have applied different tests to determine whether the disclosure of an anonymous speaker's identity is appropriate. These tests generally weigh the plaintiff's right to assert its claims against the defendant's First Amendment right to speak anonymously. For example, in *Dendrite Int'l, Inc. v. John Doe No. 3*,[51] the court developed a four-part test that requires the plaintiff to (1) notify the anonymous poster that he or she is the subject of a subpoena or application for an order of disclosure and give the defendant an opportunity to oppose the discovery requests; (2) identify each statement that allegedly constitutes actionable speech; and (3) produce evidence supporting each element of its cause of action.[52] If the plaintiff meets these requirements, the court must then "balance the defendant's First Amendment right of anonymous speech against the strength of the prima facie case presented and the necessity of the disclosure of the anonymous defendant's identity to allow the plaintiff to properly proceed."[53] In another case, *Doe v. Cahill*,[54] the court held that a defamation plaintiff could obtain the identity of an anonymous speaker only if the plaintiff takes certain steps to notify the anonymous poster regarding the subpoena, and could support his or her claim with facts sufficient to defeat a motion for summary judgment, as this standard appropriately protects First Amendment rights. Other courts have applied a less stringent "good faith" standard to determine whether the disclosure of identifying information is appropriate.[55] Regardless of the test applied, if it appears that the subpoena was requested in bad faith, and/or was an effort to "chill" a speaker's First Amendment rights, a court may quash a subpoena seeking identification of the anonymous speaker.

If the anonymous speaker is not a named party to the case, courts may apply a different test. For example, one court has set forth the following factors: "(1) the subpoena seeking the information was issued in good faith and not for any improper purpose, (2) the information sought relates to a core claim or defense, (3) the identifying information is directly and materially relevant to that claim or defense, and (4) information sufficient to establish or to disprove that claim or defense is unavailable from any other source."[56]

It is likely that similar requirements will be imposed in other situations in which one seeks to use litigation to obtain identifying information about an anonymous speaker.[57] A court, however, may be more willing to order the disclosure of identifying information about an anonymous speaker if the plaintiff's claim(s) arise out of contract law, as compared to tort claims such as defamation.[58]

***

User postings, user uploads of copyrighted materials, and subpoenas seeking user information are the three most common legal concerns of Internet publishers. For these and all other Internet legal issues, it is always wise to consult with informed counsel.

Footnotes

1 *Cubby v. CompuServe, Inc*., 776 F. Supp. 135, 139 (S.D.N.Y. 1991) (quoting *Cianci v. New Times Publ'g Co*., 639 F.2d 54, 61 (2d Cir. 1980)).

2 776 F.Supp. 135 (S.D.N.Y. 1991).

3 23 Media L.Rptr. 1794, 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995).

4 47 U.S.C. § 230(c)(1).

5 47 U.S.C. § 230(c)(2).

6 *See, e.g., Carafano v. Metrosplash.com, Inc.*, 339 F.3d 1119 (9th Cir. 2003) (providing immunity against claims of invasion of privacy, misappropriation of the right of publicity, defamation and negligence); *Doe v. Sexsearch.com*, 502 F. Supp. 2d 719 (N.D. Ohio 2007); *Chicago Lawyer's Comm. for Civil Rights Under the Law, Inc. v. Craigslist, Inc*., 461 F. Supp. 2d 681 (N.D. Ill. 2006), *aff'd*, 519 F.3d 666 (7th Cir. 2008).

7 *See, e.g., E360Insight, LLC v. Comcast Corp*., 546 F. Supp. 2d 605 (N.D. Ill. 2008).

8 47 U.S.C. § 230(c)(2).

9 146 P.3d 510 fn. 19 (2006).

10 521 F.3d 1157 (9th Cir. 2008).

11 *See, e.g*., *Zeran v. America Online, Inc.*, 129 F.3d 327 (4th Cir. 1997); *Blumenthal v. Drudge*, 992 F. Supp. 44 (D.D.C. 1998).

12 129 F.3d 327 (4th Cir. 1997).

13 More specifically, the *Zeran* decision held that liability as a "distributor" (such as was involved in *Cubby*) is a kind of "publishing" liability, and hence the Section 230 exemption for a "publisher" applies to a "distributor."

14 *Chicago Lawyer's Committee for Civil Rights Under the Law, Inc. v. Craigslist, Inc*., 461 F. Supp. 2d 681 (N.D. Ill. 2006), *aff'd*, 519 F.3d 666 (7th Cir. 2008).; *Doe v. GTE Corp.*, 347 F.3d 655 (7th Cir. 2003).

15 47 U.S.C. § 230(c)(1)(e)(2).

16 *See, e.g., Gucci Am., Inc. v. Hall & Assoc.*, 135 F. Supp. 2d 409, 413-17 (S.D.N.Y. 2001).

17 135 F. Supp. 2d 409 (S.D.N.Y. 2001).

18 *Id.*

19 *See, e.g., Perfect 10, Inc. v. CCBill, LLC*., 488 F.3d 1102 (9th Cir. 2007) ("In the absence of a definition from Congress, we construe the term 'intellectual property' to mean 'federal intellectual property'").

20 *See, e.g., Universal Commc'n Systems, Inc. v. Lycos, Inc*., 478 F.3d 413, 418 (1st Cir. 2007); *Doe v. Friendfinder Network, Inc*., 540 F. Supp. 2d 288, 299 (D.N.H. 2008); *Murawski v. Pataki*, 514 F. Supp. 2d 577, 591 (S.D.N.Y. 2007) ("Section 230(c) thus immunizes internet service providers from defamation and other, non-intellectual property, state law claims arising from third-party content").

21 *Religious Tech. Ctr. v. Netcom On-line Commc'n Servs., Inc.*, 907 F. Supp. 1361 (N.D. Cal. 1995).

22 *See, e.g., Religious Tech. Ctr.,* 907 F. Supp. at 1374 (denying defendant's motion for summary judgment on its copyright infringement claim, and stating that "[i]f plaintiffs can prove the knowledge element, [Defendant] will be liable for contributory infringement since its failure to simply cancel [Plaintiff's] infringing message and thereby stop an infringing copy from being distributed worldwide constitutes substantial participation in [Plaintiff's] public distribution of the message").

23 The DMCA only immunizes ISPs that follow its procedures from indirect liability (*i.e.*, liability for assisting the infringing acts of others) under theories of contributory infringement or vicarious liability. It does not immunize their direct copyright infringement liability. *Costar Group, Inc. v. Loopnet, Inc.*, 373 F.3d 544, 555 (4th Cir. 2004).

24 17 U.S.C. § 512(a).

25 17 U.S.C. § 512(b).

26 17 U.S.C. /§ 512(c).

27 17 U.S.C. § 512(d).

28 17 U.S.C. § 512(c)(2). A list of designated agents is available on the U.S. Copyright Office web site, at http://www.copyright.gov/onlinesp/list/index.html.

29 17 U.S.C. § 512(c)(1)(A).

30 17 U.S.C. § 512(c)(1)(B).

31 17 U.S.C. § 512(c)(1)(C).

32 *See* 17 U.S.C. § 512(j) (setting forth the scope of relief available).

33 17 U.S.C. § 512(c)(3).

34 *Id.*

35 17 U.S.C. § 512(g).

36 17 U.S.C. § 512(g)(2).

37 17 U.S.C. § 512(g)(3).

38 *Id.*

39 *Id.*

40 17 U.S.C. § 512(f); *Online Policy Group v. Diebold Inc.*, 337 F. Supp. 2d 1195 (N.D. Cal. 2004).

41 17 U.S.C. § 512(f).

42 *Online Policy Group,* 337 F. Supp. 2d at 1202.

43 572 F. Supp. 2d. 1150 (N.D. Cal. 2008).

44 17 U.S.C. § 512(i)(1); *see Perfect 10, Inc. v. CCBill, LLC*, 488 F.3d 1102 (9th Cir. 2007).

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

46 *See* "Principles for User Generated Content Services," www.ugcprinciples.com.

47 17 U.S.C. § 512(i).

48 18 U.S.C. § 2701 *et seq.*

49 *McVeigh v. Cohen*, 983 F. Supp. 215 (D.D.C. 1998).

50 *McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334, 341-42 (1995) (finding unconstitutional a state statute prohibiting anonymous publications related to elections).

51 775 A.2d 756 (N.J. App. Div. 2001).

52 *Id*. at 141.

53 *Id*. at 142.

54 884 A.2d 451, 459, 460-61 (Del. 2005). The court listed each of the elements that a defamation plaintiff must plead and ultimately prove, the last of which requires a public figure defamation plaintiff to prove that the defendant made the allegedly defamatory statements with actual malice. *Id.* at 463. The court noted that it may be difficult to satisfy this element without discovery, and stated that it did "NOT hold that the public figure defamation plaintiff is required to produce evidence on this element of the claim… In other words, a public figure defamation plaintiff must only plead and prove facts with regard to elements of the claim that are within his control." *Id*. at 464.

55 *In re Subpoena Duces Tecum to America Online, Inc.*, 2000 WL 1210372 (Va. Cir. Ct. Jan. 31, 2000) (holding that a court should enforce a subpoena and order an ISP to provide a subscriber's identity only when the court is satisfied that (1) "the party requesting the subpoena has a legitimate, good faith basis to contend that it may be the victim of conduct actionable in the jurisdiction where suit was filed," and (2) "the subpoenaed identity information is centrally needed to advance that claim").

56 *Doe v. 2TheMart.com Inc*., 140. Supp. 2d. 1088, 1095 (W.D. Wash. 2001).

57 *See also Columbia Ins. Co. v. Seescandy.com*, 185 F.R.D. 573 (N.D. Ca. 1999) (setting forth the following factors to consider before allowing discovery to obtain identifying information about a domain name registrant: the plaintiff (1) identified the missing party with specificity such that the courts can determine that defendant is a real person or entity who could be sued in Federal court; (2) identified all steps taken to locate the defendant; (3) established that its lawsuit could withstand a motion to dismiss; and (4) filed a request for discovery with the court, including reasons justifying the discovery requested and a list of persons or entities on whom discovery process might be served to provide identifying information about the defendant, thereby making service of process possible).

58 *See, e.g., Immunomedics, Inc. v. Doe*, 775 A.2d 773 (N.J. App. Div. 2001) (permitting the plaintiff to learn the identify of an anonymous speaker because her statements violated a confidentiality agreement to which she was bound).