

## Limitations on Liability Relating to Material Online: 17 U.S.C. § 512.

Function	Conduit (store and forward)	System Caching	Posting (user storage)	Linking (information location tools)	Take-down
Statutory Authority	17 U.S.C. § 512(a)	17 U.S.C. § 512(b)	17 U.S.C. § 512(c)	17 U.S.C. § 512(d)	17 U.S.C. § 512(g)*
Immunity	Partial: Monetary relief “means damages, costs, attorneys’ fees, and any other form of monetary payment.” § 512(k)(2).  Injunctive relief limited to that provided in § 512(j).	Partial: Same.	Partial: Same.	Partial: Same.	Complete: No liability: “good faith disabling of access or removal of material or activity claimed to be infringing.” § 512(g)(1).
Relief	Injunctive relief limited to (1) an order restraining access to system or network, i.e., a termination order, and (2) a blocking order: “a specified, identified, online location outside the United States.” § 512(j)(B)(i) and (ii).	Injunctive relief limited to (1) restraining order from providing access to material, (2) termination order (3), “injunctive relief as the court may consider necessary to prevent or restrain.” § 512(j)(A)(i), (ii) and (iii).	Same.	Same.	None.
Service provider must receive notice of order and “opportunity to appear” except for “preservation of evidence” or other orders not affecting operation. § 512(j)(3).					
Nature of Action	Transmission at initiation or direction of third party. Automatic technical process. No selection of recipients. Copy of material subject to access and time limits. No modification of material. § 512(a)(1)-(5).	Material available by third party. Transmission from one third party to another. Automatic technical process: “users of the system or network.”** § 512(b)(1)(A)-(C).	“Examples of such storage include providing server space for user’s web site, for a chatroom, or other forum in which material may be posted at the direction of users.” H.R. Rep. No 551 (Part 2), at p. 53; S. Rep. 105-190, at p. 43.	“The term... includes a directory or index of on-line sites or material, such as a search engine that identifies pages by specific criteria; a reference to other on-line material, such as a list of recommended sites; a pointer that stands for an Internet location or address; and a hypertext link which allows users to access material without entering its address. H.R. Rep. No 551 (Part 2), at p. 56-57; S. Rep. 105-190, p. 47.	No liability for removal or disabling if reasonable steps to promptly contact subscriber. § 512(g)(2)(A).  Subscriber option to offer a counter notice shall include “substantially”: (A) signature, ?►(B) identification of material (C) statement of good faith subject to perjury, and ?►(D) contact data and consent to jurisdiction. § 512(g)(3)(A)-(D):  Once in receipt of counter notice, service provider must contact sender of initial (c)(1)(C) notice, and offer opportunity to send second notice: sender has filed restraining order against subscriber. § 512(g)(2)(C).
Service Provider Defined	Conduit: “offering transmission, routing, or providing connections for digital online communications ... without modification.” § 512(k)(1)(A)	Same as (c).	Conduit plus: “provider of online services or network access, or the operator of facilities. therefor [sic].” Includes § 512(k)(1)(A) entity. § 512(k)(1)(B).	Same as (c).	

General Compliance Requirements	Adopt, reasonably implement a repeat infringer policy: "termination in appropriate circumstances." § 512(i)(A).  Accommodates and does not interfere with standard technical measures: owner consensus, available, no substantial cost or burden. § 512(i)(A) and (B).	Same.	Same.	Same.	If second notice not forthcoming, then service provider restores or restores within 10 to 14 business days after receipt of subscriber counter notice. § 512(g)(2)(C).  trigger copyright liability the subject of a (c)(1)(C) notice. § 512(g)(4).
Registered Agent (facilitates specific notice and take-down)	Not Required.	Not required, but recommended. Dratler, 2003, § 6.01, at 6-13.	Required. 17 U.S.C. § 512(c)(2).	Not required, but recommended. Dratler, 2003, § 6.01, at 6-13.	One who knowingly materially misrepresents is subject to damages: material or activity is infringing per (c)(1)(C), or removed or disabled in error per (g)(2) and (3). § 512(f)(1) and (2).
Name, address, phone number, and electronic mail address, and other information designated by the Register of Copyrights. § 512(c)(2)(A) and (B). 37 C.F.R. § 201.38 (\$30.00 filing fee, must file notice of change or termination). Registry available at <a href="http://www.loc.gov.copyright">http://www.loc.gov.copyright</a> .		Notice received per (c)(3): expeditiously remove or disable. 17 U.S.C. § 512(b)(2)(E).  Removal or disabling of original source material or court order to effect and statement of same § 512(b)(2)(E)(i) and (ii).	Same. § 512(c)(1)(C).	Same. § 512(d)(3).  Also receives counter-notifications from subscriber under § 512(g)(3) and second "counter" counter notifications from copyright owner under § 512(g)(2)(C).	
Elements of Notice (specific notice and take-down)		Same.	Notice must include "substantially": (i) Physical or e-signature. ▶ (ii) Identification of work infringed. ▶ (iii) Identification of infringing material. ▶ (iv) Contact information: address, telephone number, email. (v) Good faith belief. (vi) Statement of accuracy. Authorization to act subject to perjury. § 512(c)(3)(A)(i)-(vi).	Same.	
Failed notice does not trigger the knowledge of awareness standard of (c)(1)(A), however, if the three elements (marked ▶) are substantially complied with, then the notice can trigger (c)(1)(A) unless the service provider "promptly attempts to contact" the person making the notice or ("other reasonable steps to assist") in perfecting the notice. § 512(c)(3)(B)(i) and (ii).					
Special Compliance Requirements (general notice and take-down)			No knowledge or awareness, if so, expeditiously remove or disable. No financial benefit "directly" where right and ability to control exist. § 512(c)(1)(A)-(B).	No knowledge or awareness, if so expeditiously remove or disable. No financial benefit "directly" where right and ability to control exist. § 512(d)(1)-(2).	

Additional Compliance Requirements	<p>*** Under section 512(h) a copyright owner may request a subpoena from a clerk of the federal court “for identification of an alleged infringer.” “[T]he clerk <i>shall expeditiously issue</i> and sign the proposed subpoena and return it to the requester for delivery to the service provider.” § 512(h)(4). All the copyright owner or its designated agent need do is file three documents: a copy of a notification described in subsection (c)(3)(A), a proposed subpoena, and a sworn declaration to the effect that the purpose for which the subpoena is sought is to obtain the identity of an alleged infringer and that such information will only be used for the purpose of protecting rights under this title. § 512(h)(2). “The subpoena shall authorize and order the service provider receiving the notification and the subpoena to <i>expeditiously disclose</i> to the copyright owner or person authorized by the copyright owner information sufficient to identify the alleged infringer of the material described in the notification to the extent such information is available to the service provider.” § 512(h)(3).</p> <p>*** The issuance of the section 512(h) subpoena is designed to be ministerial in nature. H.R. Rep. No 551 (Part 2), 105th Cong., 2d Sess. 61 (1998); Senate Report 105-190, 105th Cong., 2d Sess. 51 (1998). The clerk must “expeditiously issue” the subpoena and the service provider must “expeditiously disclose” the identity of the alleged infringer. This process is far less costly and potentially more expedient than a court ordered subpoena under typical practices of the federal courts. However, this subpoena like all subpoenas may be challenged by a motion to quash.</p>
Additional Limitations on Liability	<p>Section 512(e) provides additional limitation on liability for institutions of higher education: Section 512(e) allows the institution to treat faculty or teaching students as a third party for conduit and cache provisions and the knowledge of the infringing faculty or student shall not be imputed to the institution for the post and link provisions. Three requirements: does not include access to online instructional material within the preceding three years, “full count” clean hands rule: no notification of infringement 3-2 (within 3 years-no more than 2 incidents of notification under (c)(3)) regarding the same faculty member and a system-wide informational compliance program (“accurately describe, and promote compliance with, the laws of the United States relating to copyright”) must be in place. § 512(e)(1)(C).</p>

Notes:

\* The immunity extended by §512(g) (immunity for liability arising from an erroneous take-down) is not immunity for copyright liability, but for defamation or unfair trade or related offenses, in other words one could not violate another’s copyright by removing an infringing work from network display, but one could defame another by suggesting that their posting (the posting that was taken down) was of a dubious (infringing) nature. See, Jay Dratler Jr., *Cyberlaw: Intellectual Property in the Digital Millennium* § 6.03[2] [a][iii][C], at 6-88—6-90 (2003) (“Presumably a service provider’s liability to its subscriber for a wrongful ‘take down’ would involve causes of action extraneous to copyright, such as breach of the subscription or account agreement, defamation (for publishing a false claim of copyright infringement), trade libel or disparagement (for similar reasons), or the like.” Id. at 6-89.).

\*\* “If this condition is interpreted narrowly as restricting the limitation on remedies to caching by a system or network for its own subscribers or account holders, it would throw a monkey wrench into the flexible and efficient operation of the Internet by discouraging caching in anticipation of requests for material by *others’* subscribers—a common and useful practice. If, on the other hand, the phrase ... covers anyone ... then the condition is not much of a limitation... The gross overdrafting of Section 512 in general, however, makes it far more reasonable to assume that Congress unintentionally included superfluous language in the statute than to conclude that Congress intended to exclude from its benefit a common practice that may indeed be the predominant caching practice on the Internet.” Jay Dratler Jr., *Cyberlaw: Intellectual Property in the Digital Millennium* § 6.03[1][a][i], at 6-46 (2003) (emphasis original and footnote omitted).

\*\*\* The dissent in *In re Charter Communications, Inc.*, 393 F.3d 771 (8th Cir. 2005), argued for a broader reading of the statute, effecting its overall purpose: “Section 512(h) authorizes a copyright owner or its representative to request a subpoena to a service provider in order to identify infringers, and the statutory definition of ‘service provider’ in § 512(k) specifically includes conduit service providers such as Charter.” Id. at 780 (Murphy, J. dissenting). “Although Charter contends that the subpoena power in the DCMA is limited by the function of the ISP, such a limitation is not to be found in a plain reading of the DMCA... If Congress had wanted to limit the type of ISP subject to a statutory subpoena, it could have easily specified that in § 512(h), but it did not.” Id. Two appellate decisions have rejected the use of the section 512(h) subpoena power against section 512(a) conduit providers. See, *In re Charter Communications, Inc.*, 393 F.3d 771(8th Cir. 2005); and *In re Verizon Internet Services, Inc.*, 351 F.3d 1229 (D.C. Cir. 2003), cert. denied 125 S. Ct. 309 (2004). See also, *In re Subpoena to University of North Carolina at Chapel Hill*, 367 F. Supp. 2d 945 (M.D. N.C. 2005). Subpoenas can issue against universities in other section 512 (cache, post and link) scenarios or under general discovery rules of procedure (Federal Civil Rule of Procedure, § 45).

- See, *Atlantic Recording Corp. v. Does 1-3*, 371 F. Supp. 2d 377 (W.D.N.Y. 2005) (Rochester Institute of Technology); and *Electra Entertainment Group, Inc. v. Does 1-9*, 2004 WL 2095581 (S.D.N.Y. 2004) (New York University).

## The Anti-Circumvention Rule and Anti-Trafficking Rules of Section 1201.

Operation	Anti-Circumvention	Anti-Trafficking	Anti-Trafficking
Section	17 U.S.C. § 1201(a)(1)	17 U.S.C. § 1201(a)(2)	17 U.S.C. § 1201(b)
Character of Control	Access	Access	Use
Prohibition	<p>Prohibits circumvention of a “technological measure that effectively controls access” to a copyrighted work.</p> <p>Circumvention: “descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair technological measure, without the authority of the copyright owner.” 17 U.S.C. § 1201(a)(3)(A).</p>	<p>Prohibits distribution of technologies that circumvent access to a copyrighted work.</p> <p>Trafficking: “manufacture, import, offer to the public, provide, or otherwise a traffic in any technology, product, service, device, component, or part thereof.” 17 U.S.C. § 1201(a)(2).</p>	<p>Prohibits distribution of technologies that circumvent use (exclusive rights) in a copyrighted work.</p> <p>Trafficking: same. 17 U.S.C. § 1201(b)(1).</p> <p>Circumvention: same. 17 U.S.C. § 1201(b)(2)(A).</p>
Definition protects a	<p>■ Effectively controls access to a work: “in the ordinary course of its operation, requires the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work.” 17 U.S.C. § 1201(a)(3)(B).</p> <p>“[M]easures that cause noticeable and recurring adverse effects on the authorized display or performance of works should not be deemed to be effective.” H.R. Rep. No. 551 (Part 2), 105th Cong. 2d Sess. 40 (1998).</p>	<p>■ Traffic (function): -- “primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access,” or has -- “limited commercially significant purpose or use other than to circumvent,” or “is marketed... for use in circumventing a technological measure that effectively controls access.” 17 U.S.C. § 1201(a)(2)(A)-(C).</p>	<p>■ Traffic (function): Same definition except “effectively right of a copyright owner under this title” replaces “effectively controls access” clause. 17 U.S.C. § 1201(b)(1)(A)-(C).</p> <p>Effectively protects a right of a copyright owner: “in the ordinary course of its operation, prevents, restricts, or otherwise limits the exercise of a right of a copyright owner under this title. 17 U.S.C. § 1201(b)(2)(B).</p>

An access or use control “device” might be something as simple as technology that prohibits viewers from fast-forwarding past advertisements on a DVD,<sup>i</sup> from playing the DVD on a PC or platform other than a DVD player,<sup>ii</sup> so-called technological handshake protocols<sup>iii</sup> and geographic use restriction codes.<sup>iv</sup>

### **Nonprofit library, archives, or educational institution 17 U.S.C. § 1201(d):**

#### ■ Requirements:

--limited retention rule, no “longer than necessary,” 17 U.S.C. § 1201(d)(1)(A);

--sole purpose of circumvention rule, “access to a commercially exploited copyrighted work solely in order to make a good faith determination of whether to acquire a copy of that work,” 17 U.S.C. § 1201(d)(1); and

--sole purpose of use rule, “good faith determination of whether to acquire,” 17 U.S.C. § 1201(d)(1)(B), see below.

■ Under (d)(2), applies only when an “identical copy of that work is not reasonably available in another form.”

■ Institution cannot use exception to engage in acts prohibited by anti-trafficking rules of 17 U.S.C. § (a)(2) or (b), i.e., no trafficking!

■ Collections must be open to public or available to researchers (similar to 17 U.S.C. § 108(a)(2)).

Under section 1203(d)(3) a nonprofit library, archives, or educational institution that “willfully for the purpose of commercial advantage or financial gain violates” the section 1201(d)(1) requirements, “shall, for the first offense, be subject to the civil remedies under section 1203,” lose its right of remission and “shall, for repeated or subsequent offenses, in addition to the civil remedies under section 1203, forfeit the exemption provided under paragraph (1).

### **Regulatory Exception pursuant to 17 U.S.C. 1201(a)(1)(D): 37 C.F.R. 201.40 (2006).**

#### ■ Six categories of works:

Audiovisual works included in the educational library of a college or university’s film or media studies department, when circumvention is accomplished for the purpose of making compilations of portions of those works for educational use in the classroom by media studies or film professors. [New category!]

Computer programs and video games distributed in formats that have become obsolete and that require the original media or hardware as a condition of access, when circumvention is accomplished for the purpose of preservation or archival reproduction of published digital works by a library or archive. A format shall be considered obsolete if the machine or system necessary to render perceptible a work stored in that format is no longer manufactured or is no longer reasonably available in the commercial marketplace. [Now limited to library and archive preservation, definition of obsolete added.]

Computer programs protected by dongles that prevent access due to malfunction or damage and which are obsolete. A dongle shall be considered obsolete if it is no longer manufactured or if a replacement or repair is no longer reasonably available in the commercial marketplace. [Same, definition of obsolete added.]

Literary works distributed in ebook format when all existing ebook editions of the work (including digital text editions made available by authorized entities) contain access controls that prevent the enabling either of the book’s read-aloud function or of screen readers that render the text into a specialized format. [Same.]

Computer programs in the form of firmware that enable wireless telephone handsets to connect to a wireless telephone communication network, when circumvention is accomplished for the sole purpose of lawfully connecting to a wireless telephone communication network. [New category!]

Sound recordings, and audiovisual works associated with those sound recordings, distributed in compact disc format and protected by technological protection measures that control access to lawfully purchased works and create or exploit security flaws or vulnerabilities that compromise the security of personal computers, when circumvention is accomplished solely for the purpose of good faith testing, investigating, or correcting such security flaws or vulnerabilities. [New.]

- i Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, Final Rule, 68 Federal Register 62011, 62015-62016 (October 31, 2003) (amending 37 C.F.R. § 201.40) (proposed class 9: “The technology which deactivates the fast-forward function of DVD players (UOP blocking) does not appear to be an access control. Nor does the record show that the “CSS, an access control used on motion pictures on DVDs, prevents the deactivation of UOP blocking. Therefore, an exemption does not appear warranted since it does not appear that access controls are preventing users from fast-forwarding on DVDs.” Id. at ).
- ii *Universal Studios, Inc. v. Corley*, 273 F.3d 429 (2d Cir. 2001) (motion picture studios place CSS encryption technology on DVDs to prevent the unauthorized viewing and copying of motion pictures).
- iii *Real Networks, Inc. v. Streambox, Inc.*, 2000 U.S. Dist. LEXIS 1889 (W.D. Wash. 2000) (preliminary injunction) (Findings of Fact 12: “The Secret Handshake is an authentication sequence which only RealServers and RealPlayers know. By design, unless this authentication sequence takes place, the RealServer does not stream the content it holds.” Findings of Fact 14: “Through the use of the Secret Handshake and the Copy Switch, owners of audio and video content can prevent the unauthorized copying of their content if they so choose.”).
- iv *Sony Computer Entertainment America Inc. v. Gamemasters, Inc.*, 87 F. Supp. 2d 976, 987 (N.D. Cal. 1999) (“Based upon the declarations before this Court, the Game Enhancer’s distinguishing feature appears to be its ability to allow consumers to play import or non-territorial SCEA video games. As discussed above, SCEA specifically designed the PlayStation console to access only those games with data codes that match the geographical location of the game console itself. The Game Enhancer circumvents the mechanism on the PlayStation console that ensures the console operates only when encrypted data is read from an authorized CD-ROM. (Pltf’s Reply at 7). Thus, at this stage, the Game Enhancer appears to be a device whose primary function is to circumvent...”).