



# Copyright Educational Series – Session V:

# DMCA Safe Harbors

---

**Mitchell Zimmerman**

**Jennifer Stanley**

FENWICK & WEST LLP

**Mountain View, California**

**mzimmerman@fenwick.com**

**(650) 335-7228**

© 2006-15 Fenwick & West LLP

**Fenwick**  
FENWICK & WEST LLP

# Digital Millennium Copyright Act

---

**DMCA (1998) = Implementing Act for  
WIPO Copyright Treaty of 1996**

**WIPO Treaty: copyright for internet age**

- ❑ **Computer program as literary work**
- ❑ **Protects databases (only per U.S. law)**
- ❑ **Outlaws circumvention of technological protection measures**
- ❑ **Outlaws deletion etc. of rights management information**

# **Digital Millennium Copyright Act Safe Harbors: 17 U.S.C. § 512**

---

## **The Safe Harbor Provisions aka DMCA Title II: Online Copyright Infringement Liability Limitation Act (OCILLA)**

- **Price extracted by telecommunications industry for agreement to DMCA and ratification of WIPO Treaties**

# Safe Harbors Effectively Protect ...

---

- Telecommunications companies, access providers, bulletin board operators, hosts, intermediaries and **“online service providers” of all kinds**
  - against serious copyright liability for infringements of hosted subscribers and others for **content is stored at the direction of users**
- PROVIDED** they (i) post a DMCA policy on website and (ii) follow take-down procedures when receive notices of infringement

# Safe Harbors ~~Effectively~~ Purport to Protect ...

---

- Telecommunications companies, access providers, bulletin board operators, hosts, intermediaries and “**online service providers**” of all kinds
- against serious copyright liability for infringements of hosted subscribers and others for **content is stored at the direction of users**

**PROVIDED** they (i) post a DMCA policy on website and (ii) follow take-down procedures when receive notices of infringement **NOT QUITE ALL THERE IS TO IT**

# Digital Millennium Copyright Act: “*Safe Harbors*”?

---

- **Conditions beyond those stated**
- **Requirements vague, complex, disputed that not clear they are really “safe harbors”**
- **Nonetheless: Must be certifiable not to set a DMCA policy in place – No downside**
  - **What the Safe Harbor provisions are / how they work**
  - **How to implement for particular clients**

## **DMCA Safe Harbors: scope of protection**

---

- **Protects eligible OSPs from monetary relief and in most cases, from injunctive relief**
- **4 Safe Harbors - each independent, and with its own criteria**
- **Liability exemptions are in addition to other defenses in copyright (or other) law**
- **Communications Decency Act § 230**

## DMCA Safe Harbors: scope of protection

---

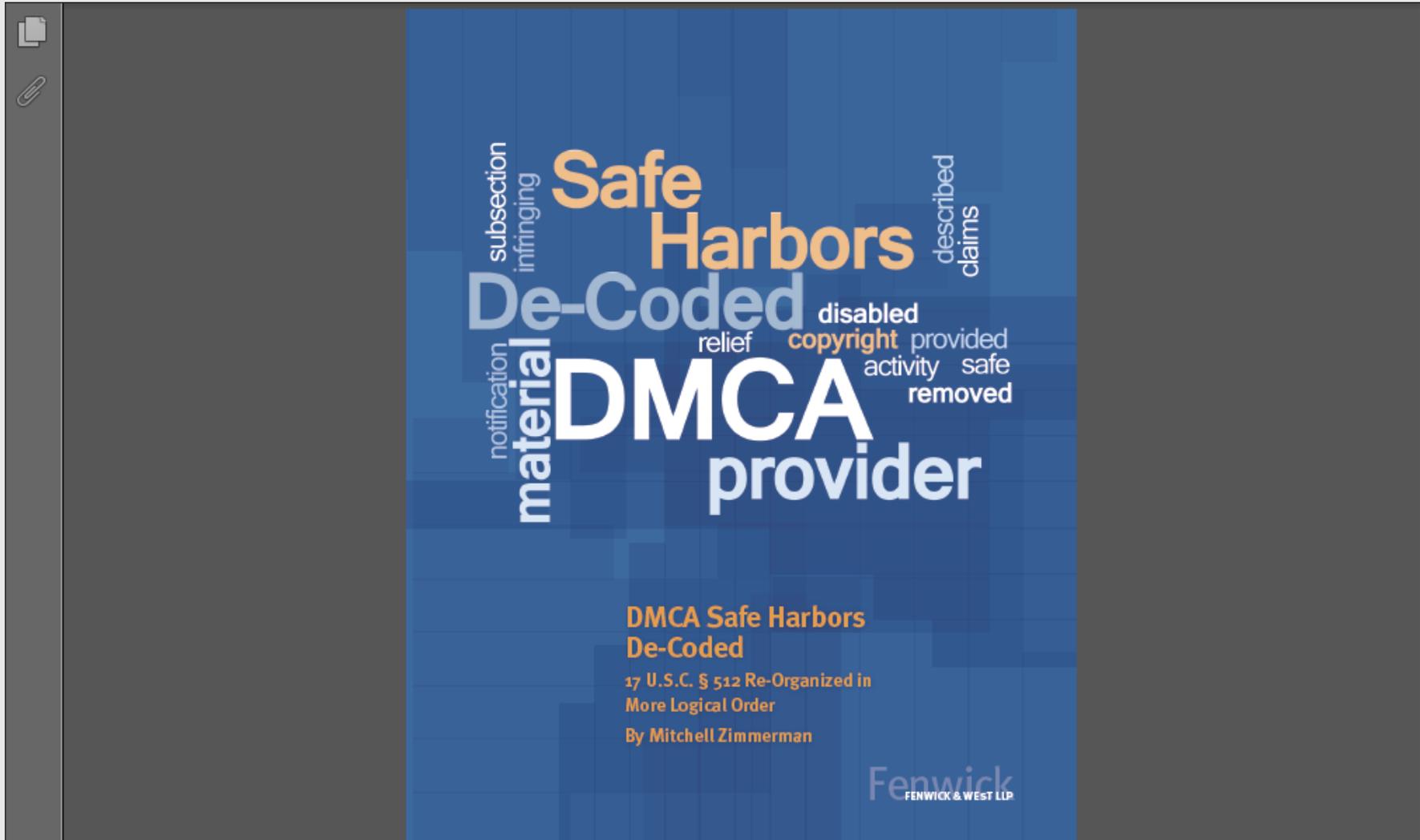
- **No such thing as “violating” DMCA**
- **Failure to meet DMCA requirements does not create liability; Plaintiff must still prove copyright infringement**

# What DMCA Safe Harbors do NOT protect against

---

- **OSP's own, direct infringing activities**
- **Acting in concert with users to create infringements**
- **Copyright claims under foreign law**
- **Liability for non-copyright infringements, such as trademark, unfair competition, rights of publicity, defamation** (But see CDA § 230)
- ***Custom:* DMCA Notice-&-Take-Down Regime = standard internationally and for IP claims generally**

# DMCA Safe Harbors De-Coded



[https://www.fenwick.com/FenwickDocuments/DMCA\\_Safe Harbors\\_De-Coded\\_05-07-12.pdf](https://www.fenwick.com/FenwickDocuments/DMCA_Safe_Harbors_De-Coded_05-07-12.pdf)

# The Four Safe Harbors

---

Two kinds of safe harbors: pertaining to role and to function:

**§ 512(a) Transitory Digital Network Communications** – Phone companies, and the like entities engaged in transmission

**§ 512 (b) System Caching**

**§ 512 (c) System Storage** – OSPs who store/transmit stuff uploaded by end-users

**§ 512 (d) Information Location Tools**  
- Search services

# Who is protected? “Service providers”

---

## *Two definitions:*

**(1) For § 512(a) Transitory Digital Network Communications – Phone companies, and the like entities engaged in transmission**

- **§ 512(k)(1)(A): “an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user’s choosing, without modification to the content of the material as sent or received”**

## Who is protected? “Service providers”

---

### *Two definitions:*

**(2) For § 512(b), (c) & (d) Everyone else (caching, storage, information location)**

- **§ 512(k)(1)(B): “a provider of online services or network access, or the operator of facilities therefor”**

**Very broad – basically all online service providers – all “services” or websites**

---

# **§ 512 (c)**

## **Storage at the Direction of Users**

## Storage-at-Direction-of-User Safe Harbor: Protects from liability for . . .

---

- **“A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright **by reason of** the storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider ...”**

**§ 512(c)(1)**

# Storage-at-Direction-of-User Safe Harbor: Protects from liability for . . .

---

## Limits injunctive relief to restraining:

- **Access to allegedly infringing materials;**
- **Access by a subscriber engaging in infringing activity, by requiring termination; and/or**
- **Other relief to restrain infringement if least burdensome to OSP**

## Storage-at-Direction-of-User Safe Harbor: Protects from liability for . . .

---

- **Interpreted to also cover activities ancillary to “storage,” including transcoding videos into different formats, and transmission – allowing users to stream and/or download videos**
  - ***UMG Recordings v. Shelter Capital / Veoh* (9<sup>th</sup> Cir. 2011)**
- **Uniformly understood to encompass website’s display of content, provided an end-user engaged in storage**

# Conditions (Precedent and Subsequent) and Disqualifiers for Storage Safe Harbor

---

- 1. Repeat Infringer Policy** (required for all safe harbors)
- 2. Accommodate** and do not interfere with “**standard technical measures**” (required for all safe harbors)

# Conditions (Precedent and Subsequent) and Disqualifiers for Storage Safe Harbor

---

- 1. Repeat Infringer Policy** (required for all safe harbors)
- 2. Accommodate and do not interfere with “standard technical measures”** (required for all safe harbors – or, actually, none)
  - **Has to do with standard measures to protect copyright agreed upon through industry-wide process / consensus**
  - **No such measures now exist within meaning of DMCA, so N/A**

# Conditions (Precedent and Subsequent) and Disqualifiers for Storage Safe Harbor

---

3. **No actual knowledge** of infringement, no “**red flags**” making infringement apparent
4. **On obtaining such knowledge, expeditiously take down** infringing matter
5. Do not have **direct financial benefit** from infringement **AND** right and ability to control
6. **Designate agent** for service of copyright claims (i) on website & (ii) in U.S. Copyright Office filing

# Conditions (Precedent and Subsequent) and Disqualifiers for Storage Safe Harbor

---

- 7. Adhere to **notice-and-take-down** regime
  - **Expediently removes on proper notice**  
**→ *Condition for further safe harbor against end-user (non-copyright) claims for wrongful take down ( § 512(g)(1))***
  - **Offer and implement counter-notice process**

# Conditions for Storage Safe Harbor: Things OSP must do to establish and maintain the safe harbor

---

## *To establish:*

**(a) Designate agent for service of copyright claims (i) on website & (ii) with U.S. Copyright Office filing**

**(b) Write and post repeat infringer policy on website**

## *To maintain:*

**(c) Set up internal processes to (i) manage notices & takedown (ii) reasonably implement repeat infringer policy**

## Different clients, Different DMCA Safe Harbor Needs

---

- **Any client that allows end-users to upload material or write comments that are posted must put a DMCA policy in place**
- **Two kinds of clients:**
  - **Those who expect very little in way of infringing material to be posted**
  - **Those who anticipate substantial part of use of site to be infringing**
- **Latter will have to devote substantial resources to dealing with infringing matter**

# Storage Safe Harbor Requirements:

## (1) Repeat Infringer Policy

---

- **Must adopt, inform users of, and reasonably implement “a policy that provides for the termination in appropriate circumstances of subscribers and account holders of the service provider's system or network who are repeat infringers” ( § 512 (i)(1)(A))**

# Repeat Infringer Policy

---

- **Example of a sufficient policy:**
  - **“It is our policy to terminate the accounts of members [users] who are repeat infringers or who are repeatedly charged with infringement in appropriate circumstances.”**
- **Subscribers must be informed of the policy, e.g.:**
  - **Refer to in Copyright Policy or Terms of Use**

# Storage Safe Harbor Requirements: (1) Repeat Infringer Policy

---

**What = reasonable implementation of policy of terminating repeat infringers in appropriate circumstances?**

- ***Ellison v. Robertson (AOL) (9<sup>th</sup> Cir.):***  
**Not reasonable implementation if email notification system does not work**

# Storage Safe Harbor Requirements:

## (1) Repeat Infringer Policy

---

### What = reasonable implementation?

- ***Napster* (9<sup>th</sup> Cir.):** Triable issue on whether reasonably implement where blocked users could reapply under another name
- ***Aimster* (7<sup>th</sup> Cir.):** Not reasonable implementation where allowing encryption makes it impossible to determine which users are transferring which files
- **BUT, *Perfect 10 v. Google*,** need not track users in any particular way

# Storage Safe Harbor Requirements: (1) Repeat Infringer Policy

---

**What = reasonable implementation?**

- ***Perfect 10 v. ccBill* (9th Cir. 2007):**
  - **“Implement” if (i) working notification system, (ii) a procedure for dealing with DMCA-compliant notifications, and (iii) don’t actively prevent copyright holders from collecting infringement info**

# Storage Safe Harbor Requirements: (1) Repeat Infringer Policy

---

**What = reasonable implementation?**

□ ***Perfect 10 v. ccBill* (9th Cir. 2007):**

- **Implement “reasonably” if in appropriate circumstances  
OSP terminates users who repeatedly or blatantly infringe**
- **Huh? “repeatedly” OR “blatantly” infringe?**

# Storage Safe Harbor Requirements:

## (1) Repeat Infringer Policy

---

- **Large complex body of cases on repeat infringement policies.**
- **Not clear whether**
  - **Receiving a notice of infringement proves user is an infringer;**
  - **Filing of a counter-notice negates a strike against the user;**
  - **Non-blatant infringers count re implementation;**
  - **OSP must make tough determinations re infringement (probably not)**

## Repeat Infringer Policy: Should client have a set of internal DMCA guidelines?

---

- **Simple, general announced policy, tracking language of statute: “It is the policy of [Company] to terminate the subscription/membership of repeat infringers in appropriate circumstances.”**
- **May also need a non-public, written set of guidelines and procedures evidencing how policy will be implemented: e.g. Three strikes – you’re out, etc.**
- **Flexibility should be built into any such process document!**

## Example of flexible, multifactor policy

---

It is the policy of [CLIENT] to terminate the accounts of repeat infringers or of users repeatedly accused of infringement in appropriate circumstances. In determining whether termination is appropriate, Company may take into account – in addition to the number of Qualifying Infringements – the following considerations among others:

- Whether the infringements were obvious or blatant, as opposed to debatable or unclear to [CLIENT]. If they were blatant, whether the user might in good faith have believed that the posted material did not infringe.

## Example of flexible, multifactor policy

---

- Whether infringing postings appear to be the mainstay of the user's postings on our web site, or just one (or a few) among myriad postings that the user has made, the great majority of which were apparently lawful.
- How many times the user has posted blatantly infringing matter, and over how long a period of time.
- How many valid notices of infringement [CLIENT] has received and acted on for this user that have resulted in take-downs, even if [CLIENT] could not easily and fairly determine the merits of the infringement claim.
- Whether the user has filed counter-notices.

## Example of flexible, multifactor policy

---

- Whether the user's other response to [CLIENT] raises a non-frivolous issue as to whether the posted content was non-infringing.
- Whether the user has some credible explanation for its offering of infringing goods, and what it may be doing to avoid a repetition of the situation.

We are not obliged to and it is not our policy to conduct an exhaustive or costly investigation before terminating a user repeatedly charged with infringement, but inasmuch as information of the above or other nature comes to our attention, the company may take that into account in determining whether termination is appropriate.

# Storage Safe Harbor Requirements:

## (2) Accommodate Standard Tech Measures

---

- (As mentioned . . . ) N/A

# Storage Safe Harbor Requirements: (3)-(4) Knowledge of Infringement, Take-Down

---

## Section 512 (c)(1)(A), (C):

- **Not eligible if OSP**
  - **actually knows that hosted material infringes, or**
  - **is aware of information making infringement apparent (red flag test)**
- **If OSP knows or is aware of the infringement, must expeditiously remove or block access**
- **(Separate obligation not requiring notice under “notice and take down” process)**

## (3)-(4) Limits on the Knowledge Bar: Defective Notices ≠ Knowledge

---

- **Copyright holder cannot rely on knowledge provided through defective notices to show knowledge negating safe harbor eligibility**
  - ***Costar Group v. Loopnet*, 373 F.3d 544 (4<sup>th</sup> Cir. 2004)**
  - ***UMG Recordings v. Shelter Capital / Veoh* (9<sup>th</sup> Cir. 2011)**

## **(3)-(4) Limits on the Knowledge Bar: No Obligation to Monitor**

---

- **§ 512 (m)(1): An OSP has no affirmative duty to monitor for or seek out possible infringements in order to be eligible for safe harbors**
- **In tension with some decisions re knowledge, turning blind eye**
- ***Custom and practice:* Sites that draw steady stream infringing content often yield to demands for screening, fingerprinting technologies**

## (3)-(4) Limits on the Knowledge Bar: Specificity of Knowledge Required

---

### What kind of knowledge is sufficient?

- **Strong trend of the cases:**

**Must be knowledge of specific instances of infringement, not general knowledge website is used by some to infringe**

***UMG Recordings v. Shelter Capital / Veoh* (9<sup>th</sup> Cir. 2011)**

**Burden for policing rests on copyright owners, not service providers; OSP bears no investigative duties (*Id.*; *ccBill.*)**

## **(3)-(4) Limits on the Knowledge Bar: Specificity of Knowledge Required**

---

### **Practice Implication of Knowledge Requirement:**

- **Operation and monitoring of website involves review, if humans who engage in monitoring see infringing stuff have to act – take-down on own**
- **Kind of site automatically generating “Favorites,” most popular: when review, take down infringers**
- **Help desk asked help with infringing stuff – No!**

# Storage Safe Harbor Requirements: (5) No Direct Financial Benefit If Right & Ability to Control

---

- **Not eligible for safe harbor if OSP has financial benefit directly attributable to the infringing activity AND the right and ability to control the infringing activity ( § 512 (c) (i) B)**

# Storage Safe Harbor Requirements: (5) No Direct Financial Benefit If Right & Ability to Control

---

- **Direct Financial Benefit:**
  - **Legis. Hist. suggests receipt of same kinds of fees from infringer and noninfringers is not direct financial benefit. “Common-sense, fact based approach.” H.R. Rep. No. 105-551 Part 2, at 54 (1998)**

# Storage Safe Harbor Requirements: (5) No Direct Financial Benefit If Right & Ability to Control

---

- **BUT “direct financial benefit” includes indirect benefit**
  - ***Napster*, 239 F.3d 1004 (9th Cir. 2001): revenue-free P2P service had “direct” financial benefit when infringing matter was draw to site, and ultimate value of enterprise rested on size of user base**
  - ***Ellison v. Robertson [AOL]*, 357 F.3d 1072 (9th Cir. 2004): “direct” benefit when infringing matter is a draw even if income from infringement not “substantial”**

# Storage Safe Harbor Requirements:

## (5) No Direct Financial Benefit If Have Right & Ability to Control

---

- **Right and Ability to Control:**

*Main line of cases ... control infringing activity, not just terminate for violating TOU*

- ***Hendrickson v. eBay Inc.*, 165 F. Supp. 2d 1082 (C.D. Cal. 2001):** ability to take down not sufficient to meet this requirement, nor does actual monitoring negate eligibility)
- ***Perfect 10 v. CCBill*, 481 F.3d 751 (9th Cir.):** mere right and ability to terminate services insufficient

# Storage Safe Harbor Requirements: (5) No Direct Financial Benefit If Right & Ability to Control

---

- **Right and Ability to Control:**
  - ***UMG Recordings v. Shelter Capital / Veoh* (9<sup>th</sup> Cir. 2011) Requires actual knowledge of specific instances of infringing matter**

# Storage Safe Harbor Requirements: (5) No Direct Financial Benefit If Right & Ability to Control

---

## Relationship of disqualifier to vicarious liability: essentially same elements

- **Vicarious liability: Underlying infringement + direct financial benefit + right & ability to control**
- **Courts split on whether safe harbor protects against vicarious liability claims**
  - ***UMG Recordings v. Shelter Capital / Veoh* (9<sup>th</sup> Cir. 2011) (“something more” than common law vicarious liability needed to vitiate safe harbor); compare *Costar Group v. Loopnet* (D.Md. 2001) (same elements, DMCA no protect against vic. liab.)**

# Storage Safe Harbor Requirements:

## (6) Designate Agent for Notification of Claims

---

- **Must designate agent for notification of copyright claims (including agent's name, physical address, phone no., and email address + info CO deems appropriate: OSP's full legal name & address, all names under which does business, agent's fax no.)**
- **Must file designation with Copyright Office (+ \$105 fee) and make same information available online at accessible part of web site (NOT users-only pages)**

## Practice Pointer: How to Designate an Agent

---

- **By role, not name of current person**
  - **E.g. copyright@company.com or DMCA@company.com or notices@company.com**
- **Make sure forwarding changes if person in role leaves or changes responsibilities**
- **Valid working email address essential or safe harbor forfeited: *Ellison v. Robertson [AOL]*, 357 F.3d 1072 (9th Cir. 2004)**

## Storage Safe Harbor Requirements: (7) Take Down and Put Back Process

---

- **If receive proper notice, OSP must**
  - **Expediently remove or block access to matter alleged to infringe &**
  - **Notify the subscriber**
  - **If notice is defective (details below), OSP may have to advise copyright holder**

## Storage Safe Harbor Requirements: (7) Take Down and Put Back Process

---

- ***Optional:* OSP may allow users to file counter-notices disputing infringement**
- **If user sends counter-notice OSP must**
  - **Promptly send copy of counter-notice to complainant**
  - **Inform complainant will restore challenged matter in 10 business days**
  - **Put challenged matter back up in 10 - 14 business days unless copyright holder files lawsuit**
- **Either way, OSP has no liability  
( § 512 (c)(3), (f), (g))**

## Storage Safe Harbor Requirements: (7) Take Down and Put Back Process

---

- **Potential for abuse:** fraudulent notices illegal and theoretically sanctionable ( § 512(f)), but can stall a competitor's marketing of challenged product because counter-notice process takes time

## **(7) Take Down and Put Back Process Counter-Notice Optional**

---

- **OSPs can (and many do) choose not to provide opportunity for counter-notice**
  - **Nonetheless immune from copyright holder claims so long as expeditiously take down allegedly infringing matter upon notice**
  - **If offer, implement and restore – exposure if safe harbor fails**

## **(7) Take Down and Put Back Process Counter-Notice Optional**

---

- **OSPs can (and many do) choose not to provide opportunity for counter-notice**
  - **Would not then be immunized against possible claims by end-user, but such claims (presumably breach of contract) could be avoided by terms of use**
  - **Something disturbing about one-sided “censorship” without notice?**
  - **Issue of user community reactions**

## **(7) Take Down and Put Back Process: Requirements of Take-Down Notice**

---

- **Written communication including substantially:**
  - 1. Physical or electronic signature**
  - 2. Identification of copyrighted works claimed to be infringed or a representative list of same**
  - 3. Identification of allegedly infringing matter to be removed and sufficient information for OSP to locate**

## (7) Take Down and Put Back Process: Requirements of Take-Down Notice

---

- **Written communication including substantially:**
  - 4. Contact information for complainant**
  - 5. Statement asserting good faith belief the use of the material is not authorized by copyright owner, its agent or the law**
  - 6. Statement that (i) above info is accurate and (ii) under penalty of perjury that complainant is authorized to act on behalf of owner of an exclusive right allegedly infringed**

## (7) Take Down and Put Back Process: Sufficiency of Notice

---

- **Substantial compliance with all requirements sufficient**
  - ***ALS Scan, Inc. v. RemarQ Communities, Inc.*, 239 F.3d 619 (4th Cir. 2001) (substantial compliance with DMCA notice requirements sufficient)**
  - ***Hendrickson v. eBay Inc.*, 165 F. Supp. 2d 1082 (C.D. Cal. 2001) (failure to include statement of belief infringing and under penalty of perjury of authority to act for copyright holder enough to hold notice defective; discusses further requirements)**

## **(7) Take Down and Put Back Process: Defective Notices**

---

### **If Notice is incomplete or non-compliant:**

- **An incomplete notice will not be admissible to show actual or “red flag” knowledge**
- **But OSP must contact the notice provider to obtain missing information if notice in substantial compliance regarding:**
  - 1. Identification of allegedly infringed work;**
  - 2. Identification of allegedly infringing material;**
  - 3. Contact info for complaining party**

## **(7) Take Down and Put Back Process: Counter Notices**

---

### **Counter Notice must include:**

- 1. Physical or electronic signature**
- 2. Identification of allegedly infringing matter that was removed and where it had been located**
- 3. Statement under penalty of perjury of good faith belief matter removed “as a result of mistake or misidentification”**  
**[mistake understood to include user’s position that positing is non-infringing]**

## **(7) Take Down and Put Back Process: Counter Notices**

---

### **Counter Notice must include:**

- 4. – User's name, address and phone no.**
  - Consent to federal district court jurisdiction where user is located or (if outside US) where OSP can be found**
  - Consent to service of process**

**OSP has no obligation to inform user of defects in counter-notice**

***Foreign posters: will be loathe to agree to be sued in USA***

## Safe Harbor eligibility intensely litigated

---

- **Was D's repeat infringer policy meaningfully implemented?**
- **Did D have knowledge of infringement?**
- **Does D have direct financial benefit + right and ability to control infringing activity?**
- **Does D respond reasonably to take-down notices?**

**Not worth litigating? But still well worth putting in place**

# Take-Down practices: Should client assist (c) holders beyond DMCA requirements?

---

## Facilitating faster notice, take-downs

- **Demands of content industries against clients whose websites host substantial amount of infringing content**
  - **Fingerprinting, other screening technologies employed at front end (i.e., monitoring)**
  - **Swift take downs**
  - **Direct access to OSP-hosted take-down tools**
- **These can be expensive**

---

# § 512 (a)

# Transmission Safe Harbor

## Transmission Safe Harbor ( § 512(a)): Transitory Digital Network Communications

---

**Eligible OSP definition different for this safe harbor:**

- **“an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user’s choosing, without modification to the content of the material as sent or received”**  
§ 512(k)(1)(A)

## § 512(a): Transitory Digital Network Protects from liability for . . .

---

- **“A service provider shall not be liable ... for infringement of copyright **by reason of** the provider’s transmitting, routing, or providing connections for, material through a system or network controlled or operated by or for the service provider, or by reason of the intermediate and transient storage of that material in the course of such transmitting, routing, or providing connections ...”**

## § 512(a): Transitory Digital Network Conditions for immunity

---

- 1. Transmission initiated by or at direction of someone else**
- 2. Transmission, routing, provision of connections or storage carried out through (i) automatic technical process (ii) without selection of material by service provider**
- 3. Service provider no select recipients except as automatic response to another's request**

## § 512(a): Transitory Digital Network Conditions

---

4. **No copy made in course of intermediate or transient storage accessible to others than anticipated recipients; and no copies maintained in manner ordinarily accessible to anticipated recipients longer than reasonably necessary for transmission, routing, or provision of connections**
5. **Material transmitted without modification of its content**

## § 512(a): Transitory Digital Network Safe Harbor

---

- **Must have repeat infringer policy – though many have no users or subscribers – and not interfere with standard technological measures**
- **NO obligation to take down or thwart access to infringing matter even when have knowledge**
- **No notice and take-down process required**

# Transmission Safe Harbor ( § 512(a)): Transitory Digital Network Communications

---

## Who is protected?

- **Phone companies**
- **Internet access services**
- **Not Napster because *inter alia* the files its users transmitted did not go through a network which it controlled, but through the Internet**
- **But some of our clients might be covered by this as well as by the storage safe harbor**

---

# Thank You!

---

# § 512 (b) Caching

## § 512(b): Transitory Digital Network Protects from liability for . . .

---

- **“A service provider shall not be liable ... for infringement of copyright by reason of the intermediate and temporary storage of material on a system or network controlled or operated by or for the service provider ...”**

**§ 512(b)(1)**

## § 512(b): System Caching Conditions for immunity

---

- 1. Material made available online by someone else [original website owner]**
- 2. Transmitted by that person through service provider's system or network at direction of someone else**
- 3. Storage through automated process for purpose of making available to yet other users who request access to the material, if following conditions satisfied:**
- 4. Material transmitted to subsequent users without modification**

## § 512(b): System Caching Conditions for immunity

---

- 5. Service provider complies with rules re refreshing, reloading, updating specified by original site, consistent with generally accepted industry protocols (unless those rules are used by original site to prevent or unreasonably impair the intermediate storage)**
- 6. Service provider no interfere with ability of technology to return (user) information that would have been available had user gone directly to original site (with some further conditions/exceptions)**

## § 512(b): System Caching Conditions for immunity

---

7. **Doesn't allow access without passwords or fees if require by original site**
8. **Take-down:** Must expeditiously take down when receive take-down notice (same as storage safe harbor) if and only if
  - i. **Infringing material has been taken down from original site and**
  - ii. **Complainant so states in notice**
9. **Repeat infringer policy required, though not clear how would be applied**

---

## § 512 (d)

# Information Location Tools

## § 512(d): Information Location Tools Protects from liability for . . .

---

- **“A service provider shall not be liable ... for infringement of copyright by reason of the provider referring or linking users to an online location containing infringing material or infringing activity, by using information location tools, including a directory, index, reference, pointer, or hypertext link ...”**

**§ 512(d)**

## § 512(d): Information Location Tools Conditions

---

- 1. Service provider lacks knowledge of infringement / no red flag, or when obtains knowledge expeditiously removes or disables access to infringing matter**
- 2. OSP does not have direct financial benefit directly AND the right and ability to control the infringing activity**
- 3. When receive notice of reference or link to infringing matter or activity, expeditiously removes link or disables access**

## § 512(d): Information Location Tools Conditions

---

- 4. Repeat infringer policy required, again, though not clear how would be applied**