Discussion Draft of the Working Group as Distributed at the Fifth Public Meeting of the Multistakeholder Forum on Improving the Operation of Notice and Takedown System on October 28, 2014

Note: The Working Group notes that this Discussion Draft is a work in progress, is subject to further comment by the Working Group and merely represents a snapshot of the Working Group discussions and work as they existed on October 28, 2014. This document will be subject to further revisions before the Sixth Public Meeting of the Multistakeholder Forum on Improving the Operation of Notice and Takedown System on December 18, 2014.

DISCUSSION DRAFT – DISCUSSION DRAFT – DISCUSSION DRAFT

USPTO DMCA Multi-stakeholder Forum

DMCA Notice-and-Takedown Processes:
List of Good Practices (Bad, and Situational Practices Being Developed)

Good

Good General Practices For Service Providers

1. Making DMCA takedown and counter-notice mechanisms easy to find and understand. There are many different ways to accomplish this, depending on the nature of the service in question, but some examples include ensuring that copyright takedown and counter-notice mechanisms appear readily in search engine results, are linked from web page headers and footers, are [included as a redirect to a particular URL – FMC to provide code to accomplish this] and/or described in Terms of Service or Help/Contact pages; [ideally we would identify a reasonable number of ways to do this and suggest them as preferred ways so that notice senders would have an idea of where to begin their search]

2. Providing a clear, "plain English" explanation (consistent with DMCA requirements) of who can submit a DMCA notice and counter-notice; what information should be submitted to comply with DMCA requirements; and what additional information, if submitted, can facilitate the removal of alleged infringing content;

3. Implementing processes that are efficient for receiving [and acting on] notices that are commensurate with the level of good faith claims of instances of infringement sought to be submitted by rights owners e.g. through
   a. allowing multiple URLs to be submitted online at one time, email, in a web form that can accommodate multiple URLs, or through upload of a text file
   b. offering, where appropriate, alternate methods of submitting notices for larger notice senders [, including, for example, scalable, machine-readable processes];
   c. Additional efficiency may be achieved by establishing a standard document structure for the email or uploaded text file.

4. For notices that meet the requirements of section 512(c)(3) and relate to infringing material, or a hyperlink to infringing material, that resides on the system or network operated by or for the service provider, providing confirmation of receipt of a notice or counter-notice that includes a method to identify the notice or counter-notice in further communications, such as a copy of the completed web form, or an email confirming that the content has been acted upon; and

5. Explaining to submitters that DMCA notices and counter-notices are only accepted to address copyright infringement claims and are not the proper method to report other legal claims (i.e. non-copyright issues such as trademark or defamation issues) or violations of community guidelines, terms of use, etc., and that there are legal sanctions that apply for certain knowing and material misrepresentations in DMCA notices.

6. [Where practicable, making reasonable efforts, following withdrawal of the notification or receipt of a counter-notification, to reinstate in a timely fashion material that has been improperly or inaccurately identified as infringing in a DMCA notice.]

For Service Providers When Email is the Submission Mechanism

1. All Good General Practices
2. TBD if add suggestion of syntax for emails or example email to make them more uniform, easier to process.

For Service Providers When a Web form is the Submission Mechanism

1. All Good General Practices

2. Web form should have clearly labeled fields and clearly mark which fields in a submission are required by the DMCA, and are therefore mandatory, and which fields are requested in order to allow for better processing of the notice (e.g where multiple works appear on a single URL or where a work such as a visual image cannot readily be identified by title/author alone);

3. Providing sample text, help buttons and instructions to help explain what information is being requested;

4. Employing industry-standard features that promote efficient submission of forms such as avoiding server-side settings that would disable browser-side auto-completion features that help submitters to easily complete fields based on prior input and employing practices similar to those used as industry standards for online sales transactions wherever possible to retain properly entered data, so the notice sender does not have to re-enter it to complete a notice if certain fields on the notice have been entered incorrectly;

5. Explaining why a notice or counter-notice submission is rejected to allow the sender to efficiently correct the submission and resubmit;

6. Implementing efficient practices for receiving notices submitted in this manner, while at the same time implementing reasonable measures to deter fraudulent, erroneous or abusive submissions.

Good General Practices for Notice Senders

1. Good faith submission of all information required by Section 512(c).

2. Submitting take down requests presented as Section 512 notices only for alleged copyright infringement.

3. Before submitting a take down notice it is a good practice to take measures that are reasonable under the circumstances (e.g. taking into account the type of service, volume and visibility of infringement, etc.) to ascertain the online location at which the alleged infringing material resides and to appropriately consider whether use of the material identified in the notice in the manner complained of is not authorized by the copyright owner, its agent or the law.

   Using automated tools of various types to search for and send notices is a common practice to improve efficiency among senders of notices who must search for numerous

works across a wide variety of sites and services and send large volumes of notices. When using these sorts of automated tools, examples of good practices include:

- Particularly where automated takedown notices will be sent to a site based on metadata (e.g. keywords, titles, file size, etc.), conducting a human review of the site to which notices will be directed to ascertain whether the site is particularly likely or unlikely to be hosting or linking to material that infringes copyright.

- Establishing search parameters the copyright owner or its agent believes will efficiently identify the unauthorized files while minimizing the inadvertent inclusion of authorized files; for example, in addition to searching on the title of the copyrighted work, using additional metadata where appropriate to help indicate whether material actually constitutes an unauthorized use of the copyrighted work. The size of the content file may be taken into account as well;

- Regularly conducting spot checks to evaluate whether the search parameters are returning the expected results, and adjusting the search parameters if needed to provide more accurate results; or

- If given sufficient information by the service provider to show that the notice sender's systems for generating notices are resulting in significant numbers of notices being sent to the service provider that do not accurately identify the online location at which the infringing material resides or that do not accurately identify the use of the material as unauthorized, making good-faith efforts to correct the issue, with assistance from the service provider as needed, when sending further notices to the service provider.]

[DISCUSS POTENTIAL FURTHER TRANSPARENCY.]

[TBD whether to include/how to address educational information for users.

Bad Practices

Bad General Practices for Service Providers

1. Intentionally obfuscating the procedure for submitting 512(c) or 512(d) take down notices or counter-notices, such as hiding contact information for submission of take down notices or counter-notices, or placing web forms or DMCA agent's email address behind multiple click-through advertisements.

2. Requiring notice and counter-notice submitters to watch advertising, or provide anything of value as a pre-condition to submitting a notice or counter-notice.

3. Using arbitrary mechanisms in a manner [intended to] make the notice or counter-notice submission process inefficient or difficult, such as use of multiple CAPTCHA codes, the use of CAPTCHA codes at the conclusion of a submission in a manner that results in the submission being lost if CAPTCHA fails, or "cool down" periods between submissions of notices or counter notices, deployed in a manner that hampers the ability of rights holders to send legitimate notices; or otherwise [using arbitrary mechanisms intended] to significantly hamper the ability of rights holders to send notices sufficient to address the scale of infringement identified on the site[; it being understood that some limits may be necessary to deter abusive practices].

4. **[TBD:** Stigmatizing or intimidating language which risks chilling submission of legitimate takedown requests or legitimate counter-notices.]

Others to be added

For Service Providers When Email is the Submission Mechanism

1. All Bad General Practices
2. [Any bad practices particular to email?]

For Service Providers When Web Form is the Submission Mechanism

1. All Bad General Practices

To be added

For UseNet Service Providers

To be added.

Bad General Practices for Notice Senders

1. Sending notices pursuant to DMCA Section 512(c) when the notice sender knows that the allegedly infringing material or activity does not reside on the service provider's system or network within the meaning of DMCA 512(c), such as when the service provider is only a 512(a) Internet access provider in the given instance **[**or the system or network is not controlled or operated by or for the service provider**]**.

2. [TBD: BAD PRACTICES RELATED TO NOTIFYING DATA CENTER OPERATORS REGARDING CONTENT THAT THEY CAN'T TAKE DOWN].

3. Falsely asserting that the notifier is authorized to act on behalf of the owner of an exclusive right asserted.

4. Submitting invalid takedown notice requests for harassing or retaliatory purposes, such as in response to a takedown notice from the alleged infringer, temporarily silencing a critic, or with the goal of disrupting the business of a competitor.

5. Submitting a DMCA take down notice to assert rights other than copyright rights.

6. Repeatedly submitting 512 notices with regard to a URL where the rights holder knows the allegedly infringing material or hyperlink has been reposted by the service provider in response to a counter-notice containing the elements set forth in § 512(g)(3). Sandra: to discuss nested links scenario where might take down links nested below.

~~6.~~7. Failing to take efforts to ensure a good faith belief that the copyrighted work identified in the notice is the work being infringed at the location identified in the notice, particularly when using automated tools tor scanning.

Comment [Halpert, 1]: Vicky and Jordan to address line between cyberlocker issue and disregard of counter-notices

~~7.~~8. Falsely asserting that the [notice sender] [rights owner] has 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~~].~~

~~8.~~9. Failing to specify in a DMCA 512(c) notice which works are infringed or where the infringing work or the hyperlink to the infringing work is located on the service provider's system or network.

Comment [Victoria 2]: TBD how/if to deal in this document with situations where this information is provided to the service provider, but not forwarded to the user.

Comment [Victoria 3]: TBD how/if to deal in this document with situations where this information is provided to the service provider, but not forwarded to the user

Bad Practices for CounterNotice Senders

Situational Practices (that Vary Based Upon the Situation/Context)

1. Trusted Submitter Programs: Discussion of potential features of these programs that further efficiency

Where practicable for a service provider to implement "trusted submitter" programs [for submitters who have a history of submitting accurate notices] can create notification efficiencies while incentivizing notifiers to follow good practices. Features of trusted submitter programs may include:

a. Log-in authentication mechanisms to verify the identity of reliable, accurate submitters;
b. Signed agreements that incorporate into each notice by reference certain information required by the DMCA that otherwise would have to be submitted each time (e.g., good faith belief, accuracy, and penalty of perjury statements);
c. Removal or appropriate adjustment of anti-abuse mechanisms such as CAPTCHA codes and volume and frequency limits for Trusted Submitters who have been authenticated;
d. Mechanisms that enable authenticated machine-to-machine submission methods, such as XML-based APIs, web form features that encourage automated submission (e.g., web forms that support text file uploads in structured formats in place of completion of web form fields); or
e. structured email formats that enable reliable, automated parsing of required information.

2.

[Acknowledgement and Status Reporting: As described above [in Section __], it is a good practice for service providers to provide confirmation of receipt of notices and a method to identify notices to facilitate further communications about particular notices. In addition, where submission scale and servicer provider resources make it practicable, the following additional measures may lead to further efficiencies in the submission process:
a. Providing submitters with a record of all URLs submitted;
b. Providing submitters with a record of the action taken with respect to a notice, consistent with privacy obligations.

a. Notices which fail to meet the requirements of section 512(c)(3) do not require and do not necessarily merit a response, although providing reasonable information to the notice sender about the deficiency of the notice (e.g. on one, but not necessarily on multiple occasions where repeated deficient notices are sent) may promote efficiency in both notice sending and processing by allowing sender errors to be corrected]

3. Requesting additional information:
    a. Requesting additional information from the notice submitter that describes the work or a link to the legitimate version can improve efficiency in certain contexts (e.g. where title information alone may not sufficiently describe the work to allow the service provider to identify the work, or where multiple copyrighted works are available at one URL and the service provider cannot locate the works because it is not clear from the notice to which work the notice refers).
    b. With respect to optional pieces of information, a service provider should consider informing notifiers that such information would encourage efficient submissions or aid in identifying the works in question (e.g. where multiple works appear on a single URL or are not readily identified by the title of the work, thus frustrating efforts by the service provider to locate the allegedly infringing work).
    c. On the other hand, care should be taken not to request additional information where the notifier provides information sufficient for the service provider [efficiently] to identify the alleged infringement.
    d. For example,

4. CAPTCHAS. Use of security measures for web form notice receiving interfaces are important and a good practice. Nevertheless, even the use of single-entry CAPTCHAs for submission of notice forms can slow down notice sending for automated take down systems as well as for individuals sending notices manually. As described above in __, use of security measures in an arbitrary fashion or in a manner [intended to] make the notice or counter-notice submission process inefficient or difficult is a bad practice. Some possible workarounds include reliance on trusted sender programs, allowing submission of a large number of URLs with a single CAPTCHA, or recourse by notice senders to submission of notices by email.

Disclaimers

These Best Practices are not intended to be, and should not be construed as, a concession or waiver with respect to any legal or policy position or as creating any legally binding rights or obligations. Stakeholders who participated in the development of these Best Practices may differ in our interpretation of relevant laws, and do not intend to resolve such differences in the Best Practices.