Department of Commerce DMCA Multistakeholder Forum

DMCA Notice-and-Takedown Processes: List of Good, Bad, and Situational Practices

I. Good Practices

A. 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, and/or described in Terms of Service or Help/Contact pages;

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[1];

3. Implementing processes that are efficient for receiving notices that are commensurate with the volume of good faith claims of instances of infringement sought to be submitted by rights owners, for example through

    a. allowing multiple URLs to be submitted online at one time, whether via email or a web form, that can accommodate multiple URLs, or via upload of a text file
    b. offering, where appropriate, alternate methods of submitting notices for to large notice senders, including, for example, scalable, machine-readable processes; and/or
    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[2] 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 notice senders that DMCA notices and counter-notices are only accepted to address copyright infringement claims and are not the proper method to report other

[1] "Allegedly Infringing content" or "allegedly infringing material," as used in this document with regard to notifications of claimed infringement, refers to material about which the notice submitter : "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." *See* 17 U.S.C. 512(c)(3)(v).

[2] Use of the word "links" or "linking" to infringements in the context of 512(d) notices in this document is also intended to encompass "referring" within the meaning of Section 512(d) ("referring … users to an online location containing infringing material or infringing activity").

legal claims (i.e. non-copyright issues such as trademark, defamation or privacy) or violations of community guidelines, terms of use, etc., and that there are legal sanctions that can apply for certain knowing and material misrepresentations in DMCA notices.

6. Making reasonable efforts, following withdrawal of the notification or receipt of a counter-notification that substantially meets the requirement of § 512(g) and where practicable, to reinstate in a timely fashion material removed pursuant to a DMCA notice.

7. If a user reposts from the same user account material that was previously removed or disabled by the service provider in response to a proper DMCA notice and the user did not submit a counter-notice in response to the DMCA notice, it is a good practice, where practicable to do so, in addition to processing the notice, for the service provider to notify the user that further reposting of the material may result in termination of the user's account.

B. Good Practices For Service Providers When Email is a Submission Mechanism

1. All Good General Practices
2. Where practicable, service providers may want to provide suggested examples of email submissions—like that in attachment A, for instance—to help notice senders send notices in a structured email format that is easier for the service provider to process.

C. Good Practices For Service Providers When a Web form is a 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 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. Displaying an error message upon rejection of a notice or counter-notice submission with an explanation to allow the submitter to efficiently correct the submission and resubmit the information to the service provider (except in the case of repeated submission of notices by a party that ignores an initial explanation);

D. 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 copyright infringement (i.e., not to address issues such as trademark, defamation, privacy, etc.).

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 information visible to the notifier and the apparent volume of infringement at the location, etc.) to determine the online location at which the material or a link to the 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 by notice senders who must search for numerous works across a wide variety of sites and services and send large volumes of notices. Use of such tools has evolved and will evolve over time. When using these sorts of automated tools, examples of current good practices include some combination of the following:

- Particularly where automated takedown notices will be sent to a site based on metadata (e.g. keywords, titles, file size, etc.), conducting, in a manner reasonable under the circumstances, 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 infringing material.

- Establishing search parameters the copyright owner or its agent believe will efficiently identify the unauthorized material while minimizing the inadvertent inclusion of authorized material; for example, in addition to searching on the title of the copyrighted work, using additional metadata (e.g. the type and size of file, etc.) where appropriate to help indicate whether material actually constitutes an unauthorized use of the copyrighted work;

- Periodically conducting spot checks to evaluate whether the search parameters are returning the expected results, and adjusting the search parameters if needed are not as expected; and/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 or a link to 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.

4. Guidelines for sending DMCA notices on behalf of other parties should be developed in accordance with these best practices.

E. Good General Practices for Counter-Notice Senders

1. Before submitting a counter-notice, taking measures that are reasonable under the circumstances, consistent with DMCA section 512(g), to determine whether the material was removed or disabled as a result of a mistake or misidentification.

II. Bad Practices

A. Bad General Practices for Service Providers (Including for Both Email and Webform Submission Methods)

1. Intentionally obfuscating the procedure for submitting DMCA 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 stigmatizing or intimidating language in connection with any DMCA notice mechanism that is intended to chill submission of legitimate notices or counter-notices.

4. For service providers that host the file associated with a link identified to the service provider in a valid DMCA notice, creating multiple links to the file with the intent of frustrating the DMCA takedown process.

B. Bad General Practices for Notice Senders

1. Sending notices pursuant to DMCA Section 512(c) or (d) when the notice sender knows that the allegedly infringing material or activity: i) does not reside on a system or network controlled or operated by or for the provider within the meaning of DMCA 512(c), or ii) is not being referred or linked to by the service provider within the meaning of DMCA Section 512(d), 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. Falsely asserting that the notifier is authorized to act on behalf of the owner of an exclusive right asserted.

3. Submitting invalid takedown notice requests for harassing or retaliatory purposes, such as in response to a takedown notice from the alleged poster of unauthorized material, temporarily silencing a critic, or with the goal of disrupting the service provider's takedown notification mechanism or the business of competitor or other person.

4. Submitting a DMCA take down notice to assert rights other than copyright rights (*e.g.*, trademark, defamation, privacy, etc.).

5. Repeatedly submitting DMCA 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 meeting the requirements set forth in § 512(g)(3).

6. Engaging in a pattern or practice of failing to take reasonable efforts under the circumstances to ascertain that the allegedly infringing material appears at or is referenced at the location identified in the notice, particularly when using automated tools tor scanning.

7. Falsely asserting that the notice submitter 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. Intentionally submitting DMCA takedown notices in bad faith in a manner intended to obfuscate the nature of the submission or cause undue delay or hardship in processing the notice (such as, for example, sending to a fax without a cover sheet; intentionally distributing elements of a 512(c) compliant takedown notice across multiple different items of correspondence, instead of including all the information in a single notice, when the notice sender has all of this information at the time of the original notice; or sending notices by mail or by fax without a name or title of the DMCA designated agent to receive notifications etc.) with the intent of making delivery the notice to the designated agent more difficult, it being understood that it is appropriate to send notices commensurate with the volume of infringing material the notice sender seeks to have removed or blocked.

9. Sending via email bulk notices as attachments in formats that cannot easily be processed by service providers, (such as an “image-only” file whose text cannot be excerpted and copied, or converted to plain text) with the intent of making response to such notices more difficult.

10. Refusing to provide the name of the notice sender and valid contact information at an online address or phone number that the notice sender checks regularly.

C. Bad General Practices for Counter-Notice Senders

1. Falsely asserting ownership of the copyrighted work identified in the DMCA notice.

2. Submitting invalid counter notices for harassing, anti-competitive, or retaliatory purposes or for monetary or other gain.

3. Failing to take reasonable efforts to form a good faith belief that the material was removed or disabled as a result of a mistake or misidentification of the identified material.

4. Falsely asserting that the submitter of the counter notice has a good faith belief that the material was removed or disabled as a result of mistake or misidentification of the identified material.

5. Failing to provide valid contact information, including, a name, telephone number and address used regularly by the counter-notifier or their representative who will accept service of process.

6. Submitting a counter-notice when a copyright infringement lawsuit has been filed by the copyright owner against the user regarding the allegedly infringing activity and the case is pending or has been decided against the user.

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

1. **Trusted Submitter Programs**: 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); and/or
    e. structured email formats that enable reliable, automated parsing of required information.

2. **Acknowledgement and Status Reporting**: 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:

    i). Providing submitters with a record of all URLs submitted;
    ii). Providing submitters with a record of the action taken with respect to a notice, consistent with privacy obligations.

    Notices which fail to meet the requirements of section 512(c)(3) do not require and do not necessarily merit providing a confirmation or record. However, providing reasonable information to the notice sender about the deficiency of the notice (e.g. on one, but not on multiple occasions where repeated deficient notices are sent) normally promotes 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 and locate the material.

4. **Security measures**, such as CAPTCHA codes or log-in-based authentication, serve an important aim for service providers that offer online submission interfaces, namely, to protect their networks from attacks or acts of malfeasance. On the other hand, mechanisms should not be deployed in a manner intended to disrupt, or make difficult, the process of sending valid notices or counter-notices. Examples of the latter would include: (a) requiring multiple CAPTCHA codes in connection with the submission of a single notice; (b) the use of CAPTCHA codes at the conclusion of a submission in a manner that results in other data entered into the form being erased if the notice sender enters the CAPTCHA incorrectly; or (c) forcing "cool down" periods between submissions in an arbitrary manner.

   It is also understood that certain security measures, including single-entry CAPTCHA requirements, can slow down the notice submission process when (a) automated systems are being used to report multiple infringements on a single system or network via an online form; or (b) a service provider only permits the submission of a single work or link via an online form before requiring the user to engage with a security measure.

   Speaking to those points, service providers, depending on the resources available and the volume of valid notices they receive, may want to consider: (a) permitting the submission of multiple, instead of single, infringements in one session under a single CAPTCHA; and (b) where appropriate, alternative methods for submission of bulk alleged infringements as identified under Good and Situational Practices.

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.