Questions for the Record from Chairman Darrell Issa for Mr. Matt Schruers
"Digital Copyright Piracy: Protecting American Consumers, Workers, and Creators"
December 13, 2023

1. **What is the correct understanding of the term "expeditiously" in the takedown provision of Section 512 of the Digital Millennium Copyright Act?**

The Digital Millennium Copyright Act (DMCA) uses the term "expeditiously" to characterize the speed with which Section 512-compliant[1] takedown notices must be processed to maintain the safe harbor.[2] What constitutes "expeditious" will naturally vary due to the size, sophistication, and technology in question. However, partnership between online service providers (OSPs) and rights holders, rather than a static legislative definition, is the key to establishing the most efficient tailored outcomes.

The U.S. Copyright Office concluded in its comprehensive 2020 report on Section 512 that the correct understanding of the term "expeditious" requires a broader circumstantial analysis:

> [C]ourts correctly recognize that a determination of expeditiousness is a fact-specific inquiry that depends on the circumstances. A standard like expeditiousness offers courts some flexibility to account for the specific circumstances surrounding the takedown notice, including technological changes that have rendered what was once expeditions [*sic*] far less so.[3]

Flexibility is a key factor in this analysis. As the U.S. Copyright Office further indicates, "Congress recognized the importance of this flexibility, stating that '[b]ecause the factual circumstances and technical parameters may vary from case to case, it is not possible to identify a uniform time limit for expeditious action.'"[4]

One reason for flexibility lies in the complexities of processing large quantities of reports in today's digital environment. When OSPs process large volumes of notices day in and out, great care is taken to appropriately address incomplete or invalid reports, fraudulent reports designed to censor legitimate speech, and other technical challenges.

Finally, flexibility is needed because each process requires differing levels of review capabilities. For example, some individual reports may contain hundreds or even thousands of pieces of content to be analyzed. It would be impractical to judge the response for this type of request against another which only requires minimal review.

---

[1] *See* 17 U.S.C. § 512(c)(3)(A).
[2] *See* 17 U.S.C. § 512(c)(1)(C).
[3] U.S. Copyright Office, *Section 512 of Title 17: A Report of the Register of Copyrights* (May 2020) at 162, https://www.copyright.gov/policy/section512/section-512-full-report.pdf.
[4] *Id.* at 162 (citing H.R. Rep. No. 105-551, pt. 2, at 53-54 (1998)); *see also* S. Rep. No. 105-190, at 44.

2. What technical, economic, or other limitations, if any, would prevent instantaneous or near instantaneous takedowns of pirated copies of works, particularly live sporting events?

There is no one-size-fits-all solution for the instantaneous takedown of content. At the outset, because only a court can adjudicate infringements, any action described here should be assumed under the context that content is *presumptively* or *allegedly* infringing.

As a general proposition, content removal processes usually depend upon the relevant system maintaining some repository of reference files, often in the form of "hashes" or "fingerprints." When such a process is in use, the system compares incoming content to these reference files and acts upon matches, perhaps by excluding or deleting matched content. Such filtering is not entirely accurate, of course, and the chosen tolerance level for determining matches will drive the amount of false positives and false negatives. These technologies are not readily compatible with live events because there is inherently no reference work which the copyright owner can provide to the streaming platform to filter against.

As I discussed in my written testimony, whether applied to fixed or live content, these technologies may raise free expression concerns if over-broadly implemented, can be prohibitively expensive, and in some cases, simply unworkable depending on the relevant system or platform. Many companies, particularly nascent ones, struggle to incorporate these technologies at scale.

Another strategy to obstruct infringing content is to use text-based navigational filtering. This filtering creates a catch-all ban on certain sites, page URLs, or links. However, automated filtering is not always effective or accurate. In particular, these technologies cannot account for context or nuance of individual uses, resulting in over-removal of non-infringing fair uses.[5] These false positives merit particular attention because any unjustified content filtering or takedown may suppress lawful expression.

Finally, it is often technically difficult to limit access to infringing content hosted elsewhere. For example, pointers to other sites may be posted by users, who promote off-site content with links or chat messages. Those types of "bread crumbs" are hard to detect, especially as features like messages and links are fundamental to the success of many sites. And, even if a responsible business were to immediately act on those infringing signals, it would not stop infringement at its source—a rogue, generally foreign, third-party site.

[5] For example, fair use might permit a user to post a clip of a sporting event while the event is still in progress. *See* Jonathan Band, *Coming to You Soon from Beijing: Misuse of the Digital Millennium Copyright Act*, Disruptive Competition Project (Jan. 20, 2022), https://www.project-disco.org/intellectual-property/012022-coming-to-you-soon-from-beijing-misuse-of-the-digital-millennium-copyright-act.

3. **In your testimony, you seemed to indicate that a distinction could (and should) be drawn between websites dedicated to piracy and websites, including websites that host user generated content, which at times have infringing material posted along with non-infringing materials. Would site blocking be an effective and reasonable tool against piracy if it were clearly limited to the former, and if so, what standard or criteria should be applied to distinguish them from the other types of sites?**

Any copyright policy designed to suppress online content should distinguish between websites dedicated to infringement and those where incidental infringement occurs by individual users. While it would be convenient for legislative action to only target foreign commercial sites that serve no purpose but infringement rather than legitimate American services with substantial non-infringing user-generated content (UGC), it is no simple task to craft site-blocking language that could accomplish this without erring on the side of over-blocking. Over-blocking at risk of silencing permissive free speech should be avoided in lieu of better detection methods that utilize appropriate tailored metrics that only remove unlawful pirated content. These methods require cooperation and data from rightsholders.

Setting aside questions of accuracy, the efficacy of site blocking is also sometimes overstated. Where blocking occurs solely through domain name system (DNS) resolution, many users learn to navigate to internet protocol (IP) addresses. And where blocking occurs at the nation-state level, many users learn to access that content through virtual private networks (VPNs). Accordingly, site blocking should not be misunderstood as furnishing a "silver bullet" solution.

4. **In your testimony, you referenced occasions where site blocking has resulted in blocking more than the intended target of the notice. Are you aware of any instances where site blocking was undertaken in another country to address piracy (not other illicit activity) and blocking of unrelated sites occurred? And if so, what was the cause of the over-breadth in each of those instances (e.g., technical limitations, errors or ambiguities in orders, human error)?**

The over-blocking examples in my testimony were attempts to address alleged piracy. These included instances in Germany and Austria involving DNS resolvers Cloudflare[6] and Quad9[7], the latter of which has since experienced this phenomenon in Italy.[8] While some witnesses at the hearing expressed the view that these examples were not pertinent to the case at hand, they are entirely on point.

In addition to the examples discussed in my testimony, CCIA members have suffered the consequences of certain site blocking measures. For example, local internet service providers (ISPs) in countries around the world have made entire services unavailable as opposed to the

[6] Alissa Starzak & Marwan Fayed, *The unintended consequences of blocking IP addresses*, The Cloudflare Blog (Dec. 16, 2022), https://blog.cloudflare.com/consequences-of-ip-blocking/; Patrick Nemeroff, *Latest copyright decision in Germany rejects blocking through global DNS resolvers*, The Cloudflare Blog (Dec. 5, 2023), https://blog.cloudflare.com/latest-copyright-decision-in-germany-rejects-blocking-through-global-dns-resolvers/.
[7] *Quad9 Turns the Sony Case Around in Dresden* (Dec. 6, 2023), Quad9, https://quad9.net/news/blog/quad9-turns-the-sony-case-around-in-dresden/.
[8] *Italian Blocking Demands: Following a Bad Example* (Dec. 6, 2023), Quad9, https://quad9.net/news/blog/italian-blocking-demands-following-a-bad-example.

handful of accounts that were engaged in the alleged piracy.[9] Some ISPs also struggle with implementing a block against specific accounts given the way certain sites operate and deliver content, usually resulting in the ISPs erring on the side of blocking entirely.[10]

[9] For example, an ISP in India blocked the entire service over a weekend because its broadcasting arm detected pirated cricket playoff matches being rebroadcast. *See Twitch Blocked in India*, Reddit (Sept. 2020), https://www.reddit.com/r/Twitch/comments/j0dghe/twitch_blocked_in_india/.

[10] For example, an entire service was blocked in Slovakia because one channel of the service was operated by a user on its prohibited website list. *See Poker streamer gets Twitch blocked for the whole of Slovakia*, Poker.org (Jun. 25, 2021), https://www.poker.org/poker-streamer-gets-twitch-blocked-for-the-whole-of-slovakia/. In another example, an ISP in Spain blocked an entire service based on a report of piracy for one specific user-operated channel. *See Twitch.tv bloqueado en España por el filtro de webs ilegales de las operadoras*, Bandanacha.eu (May 13, 2021), https://bandaancha.eu/articulos/twitch-tv-bloqueado-sistema-censura-webs-9905.