AAP | ASSOCIATION OF AMERICAN PUBLISHERS

STATEMENT OF THE
ASSOCIATION OF AMERICAN PUBLISHERS

BEFORE THE U.S. HOUSE OF REPRESENTATIVES COMMITTEE ON THE JUDICIARY SUBCOMMITTEE ON COURTS, INTELLECTUAL PROPERTY, AND THE INTERNET

On

"Digital Copyright Piracy: Protecting American Consumers, Workers, and Creators"

December 13, 2023

The Association of American Publishers (AAP) is the national trade association of the U.S. book and journal publishing industry. AAP represents the leading book, journal, and education publishers in the United States on matters of law and policy, advocating for outcomes that incentivize the publication of creative expression, professional content, and learning solutions. The U.S. publishing industry supports an extensive network of American businesses and thousands of jobs, with revenue of $28.10 billion for 2022.[1] The publishing industry is also an integral part of the broader U.S. copyright industries, which collectively added more than $1.8 trillion in annual value to U.S. gross domestic product in 2021.[2] Beyond these important economic contributions, an independent and thriving publishing industry supports the nation's political, intellectual, and cultural systems.

I. The Nature of Online Book and Journal Piracy

Certain online platforms make available, without permission from or compensation to publishers, unauthorized, infringing copies of books (consumer trade, professional books, and textbooks) and journal articles. These platforms include online distribution hubs ("cyber lockers"), auction sites, P2P technologies, apps, ecommerce platforms or marketplaces, social media platforms, and other online services that facilitate access to pirated copies of books and journal articles. Unfortunately, this infringing activity is supported, sometimes knowingly, by third-party service providers such as hosting providers, payment processing services, advertising networks, domain name registrars, and content delivery networks (CDN). While some platforms assist rights holders in mitigating the availability of infringing content, many continue to hamper the ability of publishers and other rights holders to take effective action against the infringing activity occurring on their sites or through their services. AAP has raised these concerns in prior submissions into government

[1] AAP StatShot Annual Report: Publishing Revenues Totaled $28.10 Billion for 2022 - AAP (publishers.org)
[2] *Copyright Industries in the U.S. Economy: The 2022 Report,* by Robert Stoner and Jéssica Dutra of Economists Incorporated, prepared for the International Intellectual Property Alliance (IIPA), (December 2022). https://www.iipa.org/files/uploads/2022/12/IIPA-Report-2022_Interactive_12-12-2022-1.pdf

inquiries, including in the Special 301 Out-of-Cycle Review of Notorious Markets by the Office of the U.S. Trade Representative (USTR).[3]

Over the last decade, the most egregious of these online piracy sites have included Sci-Hub and the Library Genesis network ("Libgen"). Sci-Hub has been engaged in its infringing activity since at least 2013 and continues its flagrantly infringing conduct, facilitating unauthorized access to over 88.34 million journal articles and academic papers (at least 90% of all toll access journal articles published). Sci-Hub obtains infringing copies of publishers' copyright protected works by illegally accessing the computer networks of universities, using hijacked proxy credentials (through which university personnel and students remotely access the university's intranet systems and databases). Once the operator gains access to the database, it harvests numerous articles and stores the purloined articles on its own servers, while also posting these articles to other piracy sites, including Libgen and Z-Library mirrors.[4] The site and its operator are in Russia and continue to operate with impunity. Though the site operator claims to have no knowledge of illegal tactics used to deceive legitimate subscribers into disclosing their personal credentials, there have been reported incidences of academic personnel, at university institutions whose systems have been compromised, being subjected to phishing schemes. According to the Scholarly Networks Security Initiative, Sci-Hub has compromised the networks and data of "over 400 universities and institutions across 41 countries."[5] The threat is not just to the security of university networks, or the personal data of personnel and students. The site also poses potential damage to the research process, as the site operators have no incentive to ensure the accuracy of the articles posted to the site, which may have been subject to correction, modification, or retraction. The site continues to solicit donations from users, accepting a variety of cryptocurrencies.[6] These piracy sites have reportedly also been used as the source for the content used to create training datasets for generative AI systems.[7]

In 2017 and 2015, AAP member publishers, ACS and Elsevier, secured default judgments against Sci-Hub and its operator in the United States, resulting in injunctions requiring U.S. domain name registries to suspend the site's U.S. administered domains. Unfortunately, notwithstanding these decisions, the site continues to make available and provide unauthorized access to millions of infringing copies of scientific, technical, medical, and professional journal articles into the U.S. In contrast, in the European Union, ISPs in Belgium, Denmark, France, Germany, Italy, Portugal, Spain, and Sweden are required to block access to the site, per website blocking injunctions secured by journal publishers in these jurisdictions. It is worth noting that risks to health and safety may arise when researchers, and consumers, rely on infringing articles sourced from piracy

---

[3] 2023 Review of Notorious Markets for Counterfeiting and Piracy, Submission of the Association of American Publishers, USTR-2023-0009-0020.

[4] See Petition launched for Z-Library restoration; Sci-Hub founder expresses support - The Hindu.

[5] See https://www.snsi.info.

[6] See Sci-Hub: donate.

[7] Alex Reisner, These 183,000 Books are Fueling the Biggest Fight in Publishing and Tech, The Atlantic (Sep. 25, 2023), https://www.theatlantic.com/technology/archive/2023/09/books3-database-generative-ai-training-copyright-infringement/675363/, and Revealed: The Authors Whose Pirated Books Are Powering Generative AI, The Atlantic (Aug. 19, 2023), https://www.theatlantic.com/technology/archive/2023/08/books3-ai-meta-llama-pirated-books/675063/.

sites like Sci-Hub. Publishers of scientific, technical and medical articles that report on research in these fields not only provide the infrastructure for the peer review process prior to the first publication of research outcomes, they also maintain the integrity of the scientific record by publishing the Version of Record (VoR)—i.e., the final, publisher-maintained article, continually updated and archived in consultation with the author of the article. Unlike the VoR which will reflect post-publication correction, modification, or retraction, unauthorized, infringing copies uploaded to piracy sites are unlikely to carry such corrections or retractions, and their use could potentially create serious and cascading scientific or medical errors if relied upon for further research, or even to train AI systems.

Similarly, Libgen[8] and its multiple mirror sites is a network of infringing locker sites, believed to be operated from Russia. The infringing network hosts a vast repository of infringing content — from consumer trade books, scientific, technical, and medical (STM) journal articles, technological standards, magazine articles, comic books to scholarly materials. It remains one of the most problematic piracy sites plaguing the trade, education, and STM publishing sectors. Libgen boasts that it hosts 2.4 million non-fiction books, eighty million science magazine issues, 2.2 million fiction books, two million comic strips, and magazine articles, which content is also being made available through multiple mirror sites and IPFS public gateways.[9]

II. The Harm to Authors, Publishers, and Rights Holders

The harm caused by the scale of infringing activity online—to rights holders, consumers, and the U.S. economy—has been well documented. Government reports already state that "(c)ommercial-scale copyright piracy and trademark counterfeiting cause significant financial losses for U.S. rights holders and legitimate businesses, undermine critical U.S. comparative advantages in innovation and creativity to the detriment of American workers, and pose significant risks to consumer health and safety."[10]

In addition to significant economic losses, the availability and sale of pirated materials also results in reputational harm to a rights holder's brand, reducing consumer trust in the product and the brand owner. For instance, irate consumers will return to the publisher a counterfeit or pirated book purchased from a third-party vendor on an ecommerce platform, often not knowing the book they purchased was not sourced from the publisher. In such cases, the publisher may have little choice but to shoulder the cost of the returned counterfeit or pirated book. With revenue not being fully realized by the creator, distributor, or producer of the legitimate products, rights holders may be forced to down-size their work force, resulting in lost jobs and significant harm to American workers. Further, rights holders, including publishers are forced to increase spending on anticounterfeiting and antipiracy strategies (such as retaining external monitoring and notice sending services, responding to frivolous counternotices), instead of being able to increase investment in nurturing authors and bringing new works to market. Finally, counterfeiters and pirate-producers also deprive governments of revenue that should go to funding schools,

---

[8] The site is the subject of litigation, with education publishers bringing suit in the U.S. See Cengage-v-LibGen-9-14-2023-Complaint.pdf (arstechnica.net).

[9] See Library Genesis - Wikipedia and https://www.revolutionreport.net/libgen-library-genesis/.

[10] See 2020 Review of Notorious Markets for Counterfeiting and Piracy (final).pdf (ustr.gov).

community services, and other programs as purveyors of pirated and counterfeit products do not invest in the community nor pay taxes. In addition to the health and safety risks that consumers face, when consumers browse sites that traffic in infringing content and counterfeit products, they make themselves vulnerable to malware and cyber-attacks (such as phishing), putting at risk their personal and financial information. For instance, scam (and phishing) sites may promote the availability of "free" content, but when one navigates to the site, there typically is no content for download. Instead, the site will ask the consumer to subscribe and provide credit card information. Scam sites may also utilize the (brand) name of a publishing house in its domain name, using a play-on-words, to mis-direct an unsuspecting consumer to the wrong site where their personal and financial information may be harvested.

III. The Need for Improved Remedies and Tools to Allow Rights Holders to Better Protect and Enforce Their Copyrights in the Online Environment

Despite the sophisticated nature of today's online piracy, the notice-and-takedown (NTD) system under section 512 of the Digital Millennium Copyright Act (DMCA) remains the only tool available to rights holders in the U.S., unless one has deep pockets to bring an infringement suit against the offending platform. Publishers have long noted in several submissions into government inquiries that the NTD system is no longer effective nor adequate to mitigate the nature and scale of online piracy rights holders contend with today.[11] The system perpetuates the "whack-a-mole" problem, and platform responses to takedown notifications are highly inconsistent or non-existent. Publishers and other rights holders continue to bear the significant burden in combatting online piracy, and additional tools and remedies to address large scale infringing activity more effectively and efficiently are necessary. Though the U.S. led in these areas in the past, that is no longer the case. We now need to look to processes and remedies already long available in other jurisdictions, such as a notice-and-staydown framework and a no-fault injunctive remedy, to improve the U.S. online enforcement framework.

A. Notice-and-Staydown

A notice-and-staydown framework would more adequately prevent the cyclical re-uploading of previously notified infringing content on to websites, as routinely occurs in the current NTD system. Under a staydown regime, an online intermediary — having become aware of infringing content present on its service or website — would be required to act not only to remove or disable access to that infringing content, but also to take such measures as are necessary to prevent the re-appearance of the infringing content on its site or service. Adoption of a notice-and-staydown regime would not impose upon online intermediaries a general obligation to monitor. Rather, a duty to monitor for infringing activity on their service would arise only when the online intermediary is already on notice that infringing activity is occurring. Frameworks that protect willful blindness by online intermediaries should be avoided. For example, a system that predicates action solely on actual knowledge of specific instances of infringement, typically from a notification from a rights holder. The statutory framework should clearly provide that both

[11] Section 512 of title 17: A Report by the Register of Copyrights, https://www.copyright.gov/policy/section512/section-512-full-report.pdf. The Office concluded that "the balance Congress intended when it established the section 512 safe harbor system is askew."

actual and constructive knowledge will trigger a responsibility to remove the infringing content for an online intermediary to be eligible for safe harbor protection.

AAP recommends giving serious consideration to recalibrating the knowledge standard to determine eligibility for safe harbor protection. The law should make clear that an online intermediary that is aware of infringing activity on its site or service should act expeditiously to remove or disable that infringement regardless of whether actual notice of the infringement from the copyright holder is received. Thus, if a site or service is aware of infringing content on its site, whether through actual knowledge of specific infringements or constructive knowledge of the infringing activity (i.e., from facts and circumstances that indicate or suggest infringing activity is occurring), there should arise an obligation not just to take the infringing content down or render the same inaccessible, but also a corresponding responsibility to take reasonable measures to prevent the re-appearance (re-upload) of the previously identified infringing content. As entities best positioned to prevent infringing activity online, online intermediaries should have an obligation to mitigate the infringing activity occurring on their platforms or networks, and failure to do so should give rise to consequences.

Tools are already available that would allow online intermediaries to take the necessary measures to mitigate and prevent infringing activity on their sites. The government should actively consider requiring online intermediaries to adopt technological measures — such as fingerprinting, filtering, and other content recognition technologies — that serve this purpose and were envisioned when the DCMA was adopted 25 years ago. These tools would enable online service providers to identify infringing content and prevent its appearance or reappearance on their site or service.

B. No-Fault Injunctive Remedy (Website Blocking)

The no-fault injunctive remedy, or website blocking, is available in at least forty countries. Website blocking works to disrupt piracy or large-scale copyright infringement occurring on or facilitated by blatant pirate sites located in foreign jurisdictions. In Europe, where the remedy has been available since at least 2010, over 1,800 websites and over 5,300 domains, engaged in infringing activity, have been blocked.[12] The remedy is not and has not been argued as a silver bullet to cure all online piracy ills. Rather, this remedy— as has been shown in several countries — is simply another useful tool with which to equip rights holders in their efforts to mitigate rampant online piracy more effectively and efficiently. Website blocking allows rights holders to secure an order from either a court or an administrative agency requiring ISPs to block subscriber access to sites that have little purpose other than to provide access to or traffic in infringing content online. Where the remedy exists, rights holders take great care to ensure that applications for injunctions have been brought against only the most notorious of infringing sites. Courts or the administrative agencies, before which such applications are brought, have been rigorous in their review of such applications to ensure that only egregious bad actor sites are

[12] An AAP member reports that to date, in 2023 alone, it has already detected some 1,900 pirate sites. Many of the 1,900 sites are mirrors to known pirate sites, which create the mirror or alternate sites to evade site blocking injunctions.

subject to blocking orders. This remedy has already proven effective in multiple jurisdictions around the world[13] , and a similar remedy should be adopted in the United States.

IV. Conclusion

AAP appreciates the opportunity to provide its views into the Subcommittee's inquiry into digital piracy. We note that some strategies identified in this submission, for instance, the no-fault injunctive remedy, have been available in several countries for at least a decade and have proven highly effective at disrupting piracy or large-scale copyright infringement facilitated by websites located in foreign jurisdictions. Given the nature and scale of today's online piracy, there is an urgent need for the U.S. to adopt additional meaningful tools and remedies to enable rights holders to address online piracy more effectively and efficiently. AAP stands ready to work with Congress to achieve the goal of better and more effective protection and enforcement of the intellectual property rights of American authors, publishers, and rights holders.

[13] See A Decade After SOPA/PIPA, It's Time to Revisit Website Blocking | ITIF; Website Blocking in Europe: Debated, Tested, Approved, and Defended | ITIF; and The Normalization of Website Blocking Around the World in the Fight Against Piracy Online | ITIF.