GIJLSS
Greenation International Journal of Law and Social Sciences
+62 81210467572 https://research.e-greenation.org/GIJLSS greenation.info@gmail.com
GREENATION RESEARCH

DOI: https://doi.org/10.38035/gijlss.v3i3

Video Streaming Platforms' Responsibilities for Repeated Copyright Infringement and Notice and Take Down Mechanisms

Andry Dwiarnanto[1], Megawati Barthos[2]
[1]Universitas Borobudur, Jakarta, Indonesia, andrydwiarnanto@yahoo.com
[2]Universitas Borobudur, Jakarta, Indonesia, megawati_barthos@borobudur.ac.id

Corresponding Author: andrydwiarnanto@yahoo.com[1]

Abstract: The rapid growth of video streaming platforms poses challenges to copyright protection, particularly repeated infringement by users. Although platforms act as intermediaries, the continued uploading of pirated content raises questions regarding their legal liability. This study analyzes platform responsibilities from the perspective of safe harbor and notice and take down (NTD) mechanisms based on Indonesian regulations, including the Copyright Law, the ITE Law, Government Regulation 71/2019, and Minister of Communication and Information Regulation 5/2020, and compares them with the United States' DMCA and the European Union's e-Commerce Directive & Copyright DSM Directive. The analysis shows that Indonesia has regulated platforms' obligations to take action against infringing content through NtD, but has not yet explicitly regulated the deactivation of repeat users. Regulatory strengthening is needed to balance the interests of copyright holders and users' freedom of expression, including standard NtD procedures, counter-notice mechanisms, and administrative sanctions for negligent platforms. This research is expected to contribute to policymakers and industry players in formulating adaptive regulations to the dynamics of copyright infringement in the digital era.

Keywords: Copyright, Video Streaming Platforms, Notice And Take Down, Repeat Infringement

INTRODUCTION

The phenomenon of video streaming platforms has transformed the way the public consumes and distributes audiovisual works (Anshari, 2019). The shift from traditional broadcasting to over-the-top (OTT) platforms and user-generated content (UGC)-based services has accelerated content accessibility, allowing anyone to upload clips, excerpts, or complete works within minutes (Siregar, 2025). The volume of uploads on the largest platforms is enormous; for example, some reports estimate that hundreds of hours of video are uploaded to YouTube every minute, a figure that demonstrates the scale of the content oversight problem (Gati, 2024). This intensity of uploads makes copyright issues a structural issue, not just a casual incident. Quantitative data on upload rates helps understand why conventional legal mechanisms struggle to keep up with the pace of digital distribution.

The development of new platforms with short formats and aggressive recommendation algorithms has also driven the proliferation of content involving copyrighted material (RR Ella Evrita H SE, 2025). Short video sharing apps report tens of millions of uploads daily, a reality that places moderation challenges on a different level than in the static web era (Effendi, 2024). The rapidly viral nature of content increases the likelihood of copyrighted works circulating before adequate verification mechanisms are in place. This ecosystem creates simultaneous tensions between the need for user access and the protection of creators' interests. Changes in consumer behavior and platform economic models have also altered the risk landscape of copyright infringement (Aghivirwiati, 2025).

The challenges of copyright enforcement on streaming platforms are not only quantitative but also highly technical and procedural (Setianingrum, 2025). The availability of content published across jurisdictions complicates enforcement efforts because national regulations differ, and legal proceedings may need to be conducted in multiple countries simultaneously (Tekayadi, 2025). The rapidly changing nature of electronic evidence and the ephemeral nature of some uploads complicate evidence collection. Differences in legal boundaries between countries, including exception standards and licensing, add another layer of complexity when rights holders seek to sue or request takedowns (Wibowo, 2024). Technical issues such as encryption, the use of fake accounts, and rapid re-uploads make the process of identifying infringement require an interdisciplinary approach.

The issue of user anonymity and the technical scale of uploads demonstrate that traditional enforcement methods are difficult to implement efficiently. Finding perpetrators who upload infringing material often requires international cooperation and technical assistance from service providers (Wardhana, 2024). Calculating material losses is also complicated when violations are widespread but low-intensity per incident. Alternative administrative mechanisms tend to emerge as options for a swift response, but these options raise questions regarding fair procedures and the protection of users' defense rights (Cahyono, 2025). This reality emphasizes the need to understand the theoretical framework underlying the rules on intermediaries and safe harbors before discussing platform operational liability.

The concept of intermediary liability places internet intermediaries within a specific legal framework, where certain technical activities can be exempted from direct legal liability (Hermawan, 2022). Regional legislation categorizes intermediary services into activities such as mere conduit, caching, and hosting, each of which carries terms for exemption from liability. This categorization serves to distinguish the purely technical role of transmitting data from the more active role of storing or modifying content, thus applying different legal concepts. These principles aim to balance the technical efficiency of the network with the protection of third-party rights, while avoiding liability burdens that disrupt infrastructure services (Aryani, 2024). The interpretation of each category often depends on factual elements and evidence of the service operator's behavior.

The distinction between mere conduit, caching, and hosting arises from the level of technical involvement and control over content. Mere conduit refers to activities that merely forward communications without modifying the content, thus limiting exposure to liability as long as there is no active involvement (Rauf, 2025). Caching involves temporary storage to improve transmission efficiency, but exceptions still require that the storage be technical in nature and not for the purpose of new publication (Rizaldy, 2025). Hosting involves storing content on behalf of the user, making the legal position of the host more vulnerable to prosecution if there is knowledge or failure to respond to a revealed violation (Jaya, 2024). These provisions ultimately require a standard of proof regarding "knowledge" and corrective action for the exemption from liability to be upheld.

The safe harbor principle in many legal regimes provides an umbrella of protection for service providers, provided they meet certain conditions set by law (Alfreda, 2021). This

mechanism typically links exemption from liability to the absence of specific knowledge of the violation, internal procedures for responding to claims, and prompt action upon receipt of proper notification. For example, laws governing safe harbors detail the notice-and-takedown element as a central procedure connecting rights holders with service providers. This protection also often requires internal administrative processes that can identify and address violations without compromising users' fundamental rights (Harsya, 2025). A review of these norms indicates that safe harbors are not unconditional exemptions, but rather schemes based on procedural obligations.

The technical and procedural aspects of safe harbors make notice-and-takedown provisions central to practices expected to balance interests. The procedure typically begins with a notification from the rights holder that meets the formal requirements, followed by prompt action by the service provider to remove or block access to the claimed material. Counter-notice mechanisms allow users to state legal reasons why content should remain available, and this process carries the risk of recursive burdens of proof. These provisions are usually detailed in laws or administrative guidelines to reduce legal uncertainty and mitigate the potential for abuse (Carroll, 2020). The success of such mechanisms depends on a balance between expedited procedures and guaranteed due process rights for all parties involved.

Notice-and-takedown mechanisms have not been without criticism, highlighting their potential for abuse and chilling effect on freedom of expression. These tools can be used to force the removal of legitimate content when notices are filed without a strong basis, or when service providers play it safe by withdrawing questionable material without substantiating the matter. Proactive rights holders can exploit service providers' formal obligations to file bulk claims, often leaving users and small creators facing the administrative burden of filing counter-notices. Other criticisms include a lack of transparency and limited access to a fair appeals process for users. A rational discussion of these mechanisms must consider the need for procedural guarantees that protect creators' interests while preventing the misuse of legal tools.

A comparison between the United States and European Union models reveals a shift in regulatory emphasis relevant to understanding policy options. The US model, reflected in the Digital Millennium Copyright Act, emphasizes a relatively strong safe harbor for platforms if notice-and-takedown procedures are implemented properly, a structure that supports innovation in digital services. The European Union later introduced adjustments through directives that require a different approach to content-sharing services, including provisions that place greater emphasis on the obligation to prevent the availability of content that clearly infringes copyright on certain platforms (Oktavia, 1998). This difference sparks a normative discussion about the extent to which active obligations can be imposed on service providers without compromising technical freedom and freedom of expression. A comparative analysis helps to understand the available policy options and their practical legal consequences.

Indonesian law places copyright provisions on electronic information, and regulations for the organization of electronic systems as interconnected frameworks for regulating digital content. The Copyright Law formalizes creators' exclusive rights and prohibits unauthorized reproduction, thus providing a material basis for claims against the distribution of copyrighted content. Provisions in the Law on Electronic Information and Transactions and implementing regulations, such as Government Regulation No. 71 of 2019 and Minister of Communication and Information Technology Regulation No. 5 of 2020, introduce technical and procedural obligations for electronic system operators, including mechanisms for removing prohibited information and obligations to cooperate with law enforcement. The integration of these norms demonstrates that Indonesia has the legal instruments to address problematic content, while implementation details still require further operational and normative attention.

A brief explanation of these norms confirms that each legal institution establishes a distinct role in the digital content regulatory system. Copyright provides standing for work owners to file claims, while the ITE Law and administrative regulations provide avenues for demanding content removal through administrative mechanisms and provide a legal basis for enforcement actions (Pratama, 2025). Implementing regulations address technical aspects such as service providers' obligations to provide communication channels, removal mechanisms, and access to data for law enforcement purposes. This combination of substantive and procedural norms forms a regulatory foundation that can serve as a starting point for developing more detailed policies on moderation and dispute resolution mechanisms. Areas of practical uncertainty will be the subject of further study when discussing platform responsibilities and operational practices.

METHOD

The research method used in this study is normative legal research with a statutory and conceptual approach. The statutory approach is carried out to examine applicable regulations, both at the national and international levels, which regulate safe harbors, notice-and-takedown (NtD) mechanisms, and digital platform responsibilities. The main regulations analyzed include Law Number 28 of 2014 concerning Copyright, Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions, and Regulation of the Minister of Communication and Information Technology Number 5 of 2020. For comparison, foreign legal instruments such as the Digital Millennium Copyright Act (DMCA) in the United States, the E-Commerce Directive 2000/31/EC, and the Digital Services Act 2022 in the European Union are also used. The conceptual approach is used to examine developing legal concepts related to safe harbors, repeat infringers, and copyright protection in the digital era, including the principles of due diligence, freedom of expression, and the right to information. The analysis was conducted by linking written legal norms with doctrine, international practice, and the views of legal experts, resulting in a comprehensive understanding of the effectiveness of safe harbor implementation in Indonesia. This method allows researchers not only to assess the suitability of existing regulations to practical needs but also to provide a conceptual foundation for formulating legal and policy recommendations that are more adaptive to the challenges of digital technology development.

RESULT AND DISCUSSION

Notice and Take Down & Safe Harbor Practices on Streaming Platforms

Safe harbor is a legal principle that protects internet service providers from being automatically held liable for copyright infringement by users. This concept first gained widespread recognition through the United States' Digital Millennium Copyright Act (DMCA) of 1998, specifically Section 512. This principle arose from the need to balance copyright protection with the rapid growth of content-sharing platforms in the digital world. Without a safe harbor, platform providers would face significant legal burdens due to the need to fully monitor every user upload. The normative basis of safe harbor is regulated by DMCA §512 for the United States, while the European Union regulates it through the E-Commerce Directive 2000/31/EC, updated with the Digital Services Act of 2022. Indonesia has not explicitly adopted the safe harbor concept, but its provisions can be traced to Law Number 28 of 2014 concerning Copyright, particularly Article 113 concerning criminal liability, as well as administrative provisions in Law Number 11 of 2008 concerning Electronic Information and Transactions, as amended by Law Number 19 of 2016. These regulations are reinforced by Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions and Regulation of the Minister of Communication and Information Technology Number 5 of 2020.

The main requirements for safe harbor include three main points. First, the service provider must have no actual knowledge of the violation committed by the user. Second, the service provider must act promptly to remove or disable access to the content upon receiving a valid notification. Third, service providers must not derive any direct financial benefit from the infringing activity. These three requirements are outlined in DMCA §512(c)(1), which has become the global benchmark.

The United States applies these requirements very strictly, particularly regarding the repeat infringer policy stipulated in DMCA §512(i). The European Union, through Article 14 of the E-Commerce Directive, provides similar protection for hosting providers, but does not mandate a policy of deleting repeat user accounts. The Digital Services Act 2022 updates this by adding transparency obligations and a clearer complaint mechanism. Indonesia has not yet regulated the detailed safe harbor requirements, but its approach is more administrative, with the obligation for ESOs to moderate content, as stipulated in Article 11 paragraph (1) of Minister of Communication and Information Regulation No. 5 of 2020.

Different responsibilities also arise depending on the type of internet service. The DMCA and the E-Commerce Directive divide these categories into mere conduit, caching, and hosting. Mere conduits, such as internet providers, are not responsible for the content they transmit. Caching services receive protection if they only temporarily store data for technical efficiency. Hosting services have greater obligations because they store user content on their servers, so the safe harbor applies if they meet the notice and takedown requirements.

Notice and takedown is a formal notification mechanism from copyright holders to service providers to immediately remove infringing content. This mechanism is a crucial element of the safe harbor because it indicates whether the platform acted promptly upon learning of an infringement. Without the Notice and Takedown procedure, the safe harbor cannot be implemented effectively because there is no standard for when a platform is considered negligent.

In Indonesia, copyright holders who feel aggrieved can report content to the platform by providing proof of ownership, a link to the allegedly infringing URL, and a power of attorney if represented. Article 11, paragraph (3) of the Minister of Communication and Informatics Regulation No. 5 of 2020 states that private ESOs are required to provide a complaint channel for reports of unlawful content. This mechanism is intended to provide copyright holders with a clear administrative path to enforce their rights.

Platform response deadlines are usually determined internally, but the Ministry of Communication and Informatics reserves the right to order access termination if reports are not promptly acted upon. Minister of Communication and Informatics Regulation No. Article 14, paragraph (3) of Law No. 5 of 2020 stipulates that E-Commerce Service Providers (ESPs) are required to follow up within 24 hours of a deletion request. The mechanism for counter-notifications or objections from users has not been clearly regulated, creating the potential for injustice for users who believe their content is legitimate but is unilaterally removed.

The Ministry of Communication and Informatics acts as a supervisor, based on Article 82 of Government Regulation No. 71 of 2019, which authorizes the termination of access to electronic systems containing illegal content. Article 14 of Regulation No. 5 of 2020 emphasizes that ESPs are required to comply with deletion requests from the Ministry.

This makes the Ministry of Communication and Information Technology (Kominfo) the primary actor in ensuring the implementation of the NtD, although its nature is more of an administrative control than a comprehensive legal mechanism.

The weakness of the NtD mechanism in Indonesia lies in the lack of established technical standards that guarantee transparency, accountability, and user protection. The NtD process more closely resembles administrative site blocking, as in the case of IndoXXI, rather than a legal procedure that allows for objections through counter-notices. Comparisons with

the United States and European Union models show that Indonesia places greater emphasis on the administrative obligations of ESOs, rather than an NtD system based on a balance between copyright holder rights and user freedom of expression.

Case studies are crucial for understanding how safe harbors and NtD are implemented in practice. Legal theory is often insufficient to explain the complexity of practice, as each case presents different facts, actors, and dynamics. A comparison between international and domestic cases can provide a clear picture of the challenges and regulatory gaps that need to be addressed.

The Viacom v. YouTube case in the United States courts was a landmark in testing the limits of the safe harbor. Viacom alleged that YouTube had actual knowledge that a large amount of copyright-infringing content was being uploaded to its platform but failed to promptly remove it. The court ruled that the safe harbor remains in effect as long as the platform lacks actual knowledge and promptly follows up on the takedown. This ruling underscores the importance of the actual knowledge standard in DMCA §512(c)(1).

The case of Capitol Records v. Vimeo debated the application of the repeat infringer policy required by DMCA §512(i). The court examined whether Vimeo actually had a policy of terminating the accounts of users who repeatedly infringe copyright. Issues arose regarding the extent to which platforms should actively monitor repeat infringers and how to determine the threshold for a "repeat infringer." This case demonstrated the complexity of implementing the safe harbor requirement in the real world.

The European Union also faced a landmark case in SABAM v. Netlog, decided by the Court of Justice of the European Union (CJEU). The court rejected a general monitoring obligation for all users, deeming it a violation of the right to freedom of expression. This ruling reinforced the principle that the safe harbor should not be transformed into a blanket monitoring obligation, but rather should be limited to expeditious action following a valid notification.

Administrative practices in Indonesia can be seen in the blocking of pirated streaming sites such as IndoXXI and LK21 by the Ministry of Communication and Information Technology. Blocking is carried out based on Article 40 paragraph (2b) of the ITE Law in conjunction with Article 82 of Government Regulation 71/2019. This mechanism is more similar to site blocking than NtD, as it does not involve a formal notification procedure between the copyright holder and the platform, and there is no counter-notification mechanism from users.

The repeat infringer theory in DMCA §512(i) requires platforms to have and implement a policy for terminating the accounts of users who repeatedly infringe copyright. This provision aims to prevent the misuse of the safe harbor as a shield for repeat infringers who continue to upload pirated content. This policy is also an absolute requirement for platforms to remain protected by the safe harbor.

Indonesia does not yet clearly regulate repeat infringers in the Copyright Law or the ITE Law. Platforms in Indonesia tend to simply remove infringing content based on orders from the Ministry of Communication and Information Technology without deactivating user accounts. This regulatory gap makes the safe harbor less than fully protected and raises doubts about whether Indonesia truly has a system in line with international standards.

A major challenge in implementing the safe harbor is the difficulty of identifying repeat infringers. Many users use VPNs, dynamic IP addresses, or multiple accounts to avoid detection. The burden of proof is also often debated as to whether it should be borne by the copyright holder reporting the content or by the platform controlling the system. This ambiguity reduces the effectiveness of safe harbor implementation in Indonesia.

The risk of overblocking arises when platforms remove legitimate content for fear of losing safe harbor protection. Excessive removal can interfere with freedom of expression,

especially content protected by the principles of fair use or fair dealing. The risk of underblocking occurs when the takedown system is unable to detect all violations, allowing pirated content to continue circulating. These two risks demonstrate that safe harbor requires balance to avoid new negative impacts.

The public's constitutional right to information and communication is regulated in Article 28F of the 1945 Constitution, which states that everyone has the right to communicate and obtain information. Copyright protection through safe harbor must not ignore this fundamental principle.

Analysis of Platform Liability for Repeat Infringements and Legal Recommendations

A safe harbor is a legal protection mechanism that exempts platforms from direct liability for copyright infringement committed by users. This protection aims to maintain the development of the digital ecosystem without creating excessive legal risks for service providers. However, a safe harbor is not absolute, as there are certain conditions under which it can be revoked or suspended.

A safe harbor loses its effectiveness when a platform is no longer passive but instead demonstrates active involvement in the distribution of copyright-infringing content. Revocation is also relevant when a platform is aware of a pattern of repeated infringement but fails to take adequate action. Failure to enforce a policy to disable repeat infringers' accounts and actions that facilitate the distribution of illegal content are important criteria for terminating legal protection.

International standards provide different guidelines. The DMCA in the United States, specifically 17 U.S.C. §512(i), requires a strictly enforced “repeat infringer policy.” The European Union, through E-Commerce Directive 2000/31/EC, now updated in the Digital Services Act 2022, distinguishes between neutral platforms and those that play an active role. If a platform is found to be playing an active role, the safe harbor no longer applies.

Indonesia, through Law No. 28 of 2014 concerning Copyright and Government Regulation No. 71 of 2019 concerning the Implementation of Electronic Systems and Transactions, regulates the role of electronic system administrators, but does not explicitly include a mechanism for revoking safe harbor. Consequently, international standards can serve as a reference in clarifying when legal protection for platforms should end.

Platforms have technical and policy responsibilities to prevent repeat infringements. Automatic detection technologies such as hashing, fingerprinting, and artificial intelligence function to identify content that is identical or similar to copyrighted works. These systems enable faster removal without waiting for reports from rights holders.

Retention logs, or records of user activity, are a crucial tool for tracking violation patterns. Through this data, platforms can identify accounts that repeatedly upload illegal content. A policy of terminating accounts of repeat infringers is a key pillar demonstrating a platform's commitment to enforcing copyright. Transparency in reporting on the number of content removed, the number of notifications received, and the actions taken can increase platform accountability. The public and copyright holders can assess the effectiveness of prevention efforts.

A major challenge arises from the risk of false positives when legal content is removed, as well as false negatives when illegal content escapes detection. A debate has arisen over whether full automation is appropriate, given the potential violations of freedom of expression. Article 17 of the European Union's Digital Services Act serves as a reference, as it regulates the balance between the use of automated filters and user protection mechanisms to prevent legitimate content from being blocked. Notice-and-takedown (NtD) requires clear procedures to be fair to both copyright holders and users. Standardized report formats should

include the identity of the reporter, proof of copyright ownership, the URL of the allegedly infringing content, and a statement of legal responsibility.

Platform response deadlines are key to the system's effectiveness. The DMCA provides a 24-hour to 10-day limit for responding to reports, while Indonesia does not yet have a rigid standard. The lack of a time limit clearly creates uncertainty for copyright holders and users. Counter-notices should be available as a user's right to defend themselves if they believe their content has been wrongfully removed. This mechanism can be combined with expedited dispute resolution mechanisms such as digital mediation or online arbitration to prevent all cases from having to go to court. The Ministry of Communication and Informatics plays a crucial role as a supervisor of electronic system providers based on Government Regulation No. 71 of 2019 and Ministerial Regulation No. 5 of 2020. However, the current supervisory function is still more focused on blocking sites rather than systematically managing the NtD system. A revision of Law No. 28 of 2014 is needed to provide clearer regulations regarding repeat infringers. Platforms should be required to deactivate accounts after a certain number of proven violations.

Minimum technical standards for electronic system providers need to be outlined in implementing regulations. These standards include activity logging, due diligence obligations, active collaboration with copyright holders, and the publication of periodic transparency reports. Administrative sanctions can be imposed on platforms that fail to comply. Warnings, fines, and even blocking access can be options for enforcing obligations without always relying on criminal or civil sanctions. A hybrid safe harbor model is worth considering. This model provides legal protection for platforms that meet due diligence standards, but revokes protection if proven negligent. This approach has been implemented in various jurisdictions, including the United States through the DMCA and the European Union through the Digital Services Act, and could be enhanced by practices from Asian countries like South Korea and Japan.

The balance between copyright protection and freedom of expression is a key issue. Overblocking can cause legitimate content to be removed, thus disrupting the public's right to access information. Article 28F of the 1945 Constitution guarantees the right to obtain information and to communicate, so it is important to ensure that the copyright enforcement system does not restrict citizens' freedoms. The risk of underblocking is also real when repeated infringements remain unaddressed due to weak detection systems. This situation is detrimental to copyright holders and undermines trust in the law enforcement system.

Business competition is also impacted by the implementation of upload filters. The high costs required to implement this system can burden local startups, while large global companies are better able to cope. This imbalance in competitiveness has the potential to lead to the dominance of big tech in Indonesia's digital market. Policies need to be designed to maintain competitive fairness. Regulations must prevent the creation of barriers to market entry for small and medium-sized companies. Technical obligations should be proportionate to the scale of the platform to avoid stifling digital innovation. The chilling effect on innovation is also worth noting. When regulations are too strict, digital business actors tend to be overly cautious, which can slow down the dynamics of technological development. Indonesia needs to find a formula that balances copyright protection, freedom of expression, and the sustainability of digital innovation.

CONCLUSION

Safe harbors still serve as a legal protection instrument that provides certainty for digital platforms, including video streaming services, so they are not immediately held liable for copyright infringement committed by users. However, the effectiveness of this scheme has proven to be limited when dealing with cases of repeat infringement. Law No. 28 of 2014

concerning Copyright and Government Regulation No. 71 of 2019 concerning the Implementation of Electronic Systems and Transactions do recognize the role of electronic system administrators, but they do not specifically regulate platform obligations to prosecute repeat infringers. This legal loophole has the potential to weaken copyright enforcement, as negligent platforms can still seek refuge behind safe harbor status. A comparison with the DMCA (US) and the Digital Services Act (EU) standards shows that safe harbors should be revoked when a platform is aware of a pattern of repeat infringement or is actively involved in the distribution of infringing content. Therefore, safe harbors are not absolute protection but are conditional on due diligence.

Strengthening a safe harbor-based copyright enforcement system requires a combination of legal and technical policies. Priorities that need to be adopted include mandatory account deactivation for repeat infringers, the establishment of measurable and clear notice-and-takedown (NtD) standards, the implementation of mandatory transparency in content removal reports similar to the DMCA mechanism, and effective administrative sanctions for electronic system operators who neglect them. These policies must be designed proportionally so as not to compromise user human rights, particularly freedom of expression and the right to information. To support regulatory effectiveness, further empirical research is needed, such as measuring the repetition of many infringements in Indonesia, evaluating the effectiveness of automatic detection algorithms, and their impact on digital market competition. Future legal studies could focus on analyzing court decisions related to digital copyright disputes, surveying rights holders and platforms, and piloting rapid remedial mechanisms based on online mediation. The results of this further research will strengthen the foundation for policymakers in developing regulations that balance copyright protection, the public interest, and the sustainability of digital innovation in Indonesia.

REFERENCES

Anshari, I. N. (2019). Sirkulasi Film dan Program Televisi di Era Digital: Studi Kasus Praktik Download dan Streaming melalui Situs Bajakan. *Komuniti: Jurnal Komunikasi dan Teknologi Informasi, 10*(2), 88-102.

Siregar, A. R. (2025). TRANSFORMASI KEBIJAKAN PENYIARAN DI ERA DIGITAL ANALISIS DAMPAK REGULASI OVER-THE-TOP (OTT) TERHADAP INDUSTRI TELEVISI KONVENSIONAL. *FIKRUNA: Jurnal Ilmiah Kependidikan dan Kemasyarakatan, 7*(3), 846-868.

Gati, R. S. (2024). *Jurus Ampuh Menjadi Konten Kreator di Youtube, Instagram, dan Tiktok: Panduan dari Nol hingga Monetisasi.* Yogyakarta: DIVA PRESS.

RR Ella Evrita H SE, M. M. (2025). *Digital Darwinism: Hukum, Kreativitas, dan Evolusi Media di Era AI.* Jakarta: PT Indonesia Delapan Kreasi Nusa.

Effendi, V. N. (2024). Analisis Konten Media Sosial Instagram Bengkulu Info Sebagai Media Penyebaran Informasi Lokal. *Harmonization: Jurnal Ilmu Sosial, Ilmu Hukum, dan Ilmu Ekonomi, 2*(2), 67-82.

Aghivirwiati, G. A. (2025). *EKONOMI DIGITAL DAN PERUBAHAN STRUKTUR PASAR.* Batam: Cendikia Mulia Mandiri.

Setianingrum, R. A. (2025). Monetisasi karya digital dan tantangan perlindungan hak cipta di indonesia. *Jurnal Ekonomi dan Bisnis Digital, 2*(4), 2683-2687.

Tekayadi, S. S. (2025). Tantangan Penegakan Hukum Siber Di Era Lintas Negara Dan Upaya Harmonisasi Global. *Jurnal Risalah Kenotariatan, 6*(1), 265-276.

Wibowo, M. S. (2024). Kendala teknis dan hukum dalam proses penyidikan tindak pidana siber di Indonesia. *Jurnal Hukum Lex Generalis, 5*(7).

Wardhana, A. W. (2024). PARADIGMA KEBEBASAN BERPENDAPAT: ANONIMITAS, BUDAYA PARTISIPASI, DAN DOMINASI SUBYEKTIFITAS PENGETAHUAN DI RUANG DIGITAL. *Jurnal Abdi Insani, 11*(1), 913-922.

Cahyono, S. T. (2025). RIKONSTRUKSI HUKUM PIDANA TERHADAP KEJAHATAN SIBER (CYBER CRIME) DALAM SISTEM PERADILAN PIDANA INDONESIA: Rekonstruksi Hukum Pidana terhadap Kejahatan Siber (Cyber Crime) dalam Sistem Peradilan Pidana Indonesia. *Dame Journal of Law, 1*(1), 1-23.

Hermawan, A. W. (2022). Secondary Liability and Safe Harbors for Platform Providers in Indonesian E-Commerce Law. *Scientium Law Review (SLR), 1*(3), 101-108.

Aryani, R. (2024). Analisis hukum tentang tanggung jawab pihak ketiga dalam investasi infrastruktur. *Jurnal Intelek Dan Cendikiawan Nusantara, 1*(2), 1078-1088.

Rauf, A. A. (2025). Tanggung Jawab Hukum Penyedia Layanan Internet Terhadap Konten Ilegal Di Dunia Maya. *SISITI: Seminar Ilmiah Sistem Informasi dan Teknologi Informasi, 14*(1), 48-56.

Rizaldy, I. R. (2025). Penilaian Berbasis Data Terhadap Skalabilitas Blockchain, Keamanan Kriptografi, Dan Adopsi Kriptokurensi Mengukur Tren Pasar Dan Dampak Implementasi Industri. *Jurnal Intelek Dan Cendikiawan Nusantara, 2*(4), 4736-4731.

Jaya, N. I. (2024). Privacy Violations in Live Streaming Pose Significant Legal Challenges Globally. *Indonesian Journal of Law and Economics Review, 19*(3), 10-21.

Alfreda, I. J. (2021). Pelindungan dan tanggung jawab kebocoran informasi pada penyedia platform digital berdasarkan perspektif rahasia dagang. *Jurnal Sains Sosio Humaniora, 5*(1), 1-16.

Harsya, R. M. (2025). Tinjauan Yuridis terhadap Tanggung Jawab Platform Digital atas Konten Ilegal Menurut Hukum Indonesia. *Sanskara Hukum dan HAM, 4*(01), 276-286.

Carroll, M. W. (2020). Copyright's Creative Hierarchy in the Performing Arts. *Vanderbilt Journal of Entertainment and Technology Law, 14*, 797 https://scholarship.law.vanderbilt.edu/jetlaw/vol14/iss4/1.

Oktavia, A. J. (1998). PENGATURAN SAFE HARBOR DAN PRIVACY SHIELD DALAM PERLINDUNGAN DATA PRIVASI DI UNI EROPA DAN AMERIKA SERIKAT. *PROSIDING*, 208.

Pratama, R. R. (2025). Hubungan Hukum Terhadap Kepemilikan Hak Cipta Yang Dijadikan Merek Bagi Pencipta Dan Pemegang Merek. *Jurnal USM Law Review, 8*(1), 65-85.