MASALAH-MASALAH HUKUM
Available online on https://ejournal.undip.ac.id/index.php/mmh/
Volume 54, Issue 3, November 2025

COMPARATIVE ANALYSIS OF PLATFORM LIABILITY FOR ILLEGAL PREMIUM ACCOUNT SALES: A STUDY OF SAFE HARBOR PRINCIPLES IN INDONESIA AND THE UNITED STATES

Ni Putu Ayu Meylan Ardini[1]*, Ni Ketut Supasti Dharmawan[1], Salwa Putri Hardiyan[2]
[1]Faculty of Law, Universitas Udayana, Denpasar, Indonesia
[2]University of Birmingham, Birmingham, England, United Kingdom
*putu.meylan03@gmail.com

Abstract

The rapid development of Indonesia's digital economy has created new opportunities but also significant challenges, particularly regarding the illegal sale of shared premium accounts on e-commerce platforms. This study examines the legal frameworks governing platform liability for these illegal activities, comparing Indonesia's regulations with the United States' Digital Millennium Copyright Act (DMCA). Using a doctrinal legal research method, the research focuses on key Indonesian laws such as the Copyright Law (Law No. 28 of 2014) and the Information and Electronic Transactions Law (ITE Law), alongside Section 512 of the DMCA. The study finds that Indonesia's legal framework provides only implicit protections, relying on general principles like good faith and fault-based liability, which leads to legal uncertainty. In contrast, the United States' DMCA offers clearer protections through its Safe Harbor provisions, including a specific notice-and-takedown procedure. This comparative analysis highlights the vulnerability of Indonesian platforms to lawsuits and the broader economic consequences, such as lost revenue, hindered innovation, and potential reputational damage. Furthermore, it emphasizes the need for clearer, consolidated regulations in Indonesia to effectively protect copyright holders and digital platforms. The study proposes a Sui Generis Safe Harbor Model that combines the procedural clarity of the DMCA with Indonesia's civil law tradition, including the establishment of clear Red Flag Knowledge standards, a mandatory notice-and-takedown procedure, and data disclosure requirements. The research underscores the importance of regulatory reform, enhanced law enforcement coordination, and technological investment to address illegal premium account sales and secure a fair digital environment.

Keywords: Safe Harbor; Digital License; Copyright; E-Commerce; Premium Account.

A. Introduction

The development of Indonesia's digital economy has recently seen a significant surge, particularly concerning the country's economic growth (Meidyasari, 2024). The reasons for this are a considerably large population and the increasingly widespread and rapid improvement of internet access (Hildawati et al., 2024). Within Southeast Asia, Indonesia has the opportunity to become a major force in the digital economy (Avirutha, 2021). This opportunity spans various sectors, including financial technology services, e-commerce, application-based transportation, and educational technology. This phenomenon is not only seen as creating new economic opportunities but also as a factor transforming how society conducts transactions, such as using electronic money, and interacts within it (Junaedi et al., 2022). The global economic transformation, including in Indonesia, has been primarily driven by the role of the digital economy as a major catalyst. Subsequently, in 2021 and 2022, Indonesia experienced economic

recovery and strong growth, even showing positive trends compared to the previous year (Cahyono et al., 2023). The development of the digital economy in Indonesia is progressing very rapidly. It is estimated that the digital economy sector will contribute more than 40% to national economic growth by 2023.

The digitalization of MSMEs is one of the driving factors. MSMEs that transition to digital platforms, such as Tokopedia and Shopee, are able to increase their revenue and market reach (Purba et al., 2025). Various industries, including retail, have undergone a major transformation as a result of the digital era. The basic concept or plan that describes how a company's strategic business framework generates revenue and profit is called a business model (Setiawan et al., 2023). A business model outlines revenue sources, target markets, cost structures, and how the company creates value for its customers. The variation in business models is vast, depending on the type of business and the strategy applied. The subscription business model is a strategy where customers pay a recurring fee usually monthly, annually, or for another period to gain continuous access to a product or service (Ekawijaya et al., 2023). Customers commit to being long-term patrons, allowing the business to secure a stable and predictable revenue stream. Thus, the subscription business model is not only considered a revenue strategy but also a way to build long-term customer relationships, advance the business as a whole, and increase loyalty (Puspita S et al., 2024). Various companies can utilize their sites by implementing a subscription system for consumers to be granted full access to the content on the application (Hildawati et al., 2024).

The impact of advancing technology continues to be felt through the convenience it offers everyone in various applications. For instance, applications like Spotify, Viu, Netflix, Canva, YouTube, and others provide easier access to their features through subscriptions (Sawitri & Dharmawan, 2021). The benefits of subscribing, such as access to provided services, can be easily obtained by people anywhere and anytime. According to Kotler & Keller, consumer behavior is the activity related to the process of selecting, purchasing, and using a product by consumers to fulfill their wants and needs (Syafrianita et al., 2022). There is an economic principle that continues to influence consumers: “to achieve the greatest benefit with minimal effort/expenditure.” However, it is noticeable that the distribution of premium application services on platforms is widespread and easily obtainable illegally. It should be noted that the illegal distribution of premium application services is very extensive. Consumers are certainly attracted because the quality is no different or lower than the legal version and is obtained at a more affordable price than the service offered on the official platform. Problems can certainly arise from this in the future (Achya et al., 2023).

Based on Article 28 of Law No. 28 of 2014 concerning Copyright (Copyright Law), the commercial use of a copyrighted work is permitted for the creator or copyright holder who obtains permission from the creator (Abduh & Fajaruddin, 2021). Nevertheless, violations of this rule are often committed by parties who do not comply with the applicable provisions. Such violations are carried out through the duplication, distribution, and sale of shared premium accounts on e-commerce, as well as the exploitation of these rights for personal gain. The issue of protecting premium platform features must be given more attention to prevent misuse by other parties (Salsabila et al., 2025). The widespread impact of online commerce has resulted in various forms of digital platforms and diverse regulations. Several countries have established separate regulations regarding the accountability of platforms as providers of trade through electronic systems. One such country is the United States, through the provisions of the Digital Millennium Copyright Act (DMCA).

The DMCA is a legal provision effectively designed to regulate the relationship between copyright and the rapid development of the internet in the United States (Nurullayev, 2023). The DMCA is a cornerstone legal provision specifically designed to reconcile copyright protection with the rapid development of the internet by providing a safe harbor for online service providers (OSPs) under certain conditions (Thakur, 2024). DMCA was designed in Congress to update

United States copyright law to align with the technological advancements of the internet in the late 1980's (Parmadi, 2024). Its purpose is to protect copyright holders' rights and give them a measure of security, while shielding online platforms from liability through safe-harbor provisions. The DMCA is organized into five titles: Title I — the WIPO Copyright and Performances and Phonograms Treaties Implementation Act of 1998; Title II — the Online Copyright Infringement Liability Limitation Act; Title III — the Computer Maintenance Competition Assurance Act; Title IV — Miscellaneous Provisions; and Title V — the Vessel Hull Design Protection Act. The DMCA also added three provisions to existing U.S. copyright law: Sections 1201, 1202, and 512. This article focuses on Section 512, which enables copyright owners to have infringing content removed without initiating litigation and provides legal protection (a "safe harbor") to online service providers that cooperate with rights holders and meet certain statutory requirements. Section 512 is the most frequently discussed part of the DMCA because it defines the obligations and eligibility criteria that service providers must satisfy (Ortega, 2023).

Safe Harbor is a legal principal that provides protection or limitation of liability from legal action for certain parties, especially platform providers or electronic system providers (ESP), as long as they have met a set of predetermined conditions (Pratama, 2017a). Its main purpose is to protect platform providers from faults or violations committed by their own users, such as copyright infringement or the uploading of illegal content (Ramadhanty et al., 2020). This protection is not absolute but conditional. A platform can be exempt from legal responsibility if it takes specific proactive steps. These include informing users of its copyright policy to prevent infringement, being aware of the infringement through actual knowledge or circumstances that make the infringement apparent, and promptly removing the infringing material once it becomes aware of it. Additionally, the platform must not receive direct financial benefits from the infringement while having the ability to control the infringing activity. It must also appoint an agent to receive claims and comply with notices from authorized government bodies, ensuring the removal of infringing content and adopting appropriate technology to manage the removal or blocking of access with proper notification (Ramadhanty et al., 2020).

The application of the safe harbor doctrine is highly relevant in various cyber law contexts, both in Indonesia and globally. In Indonesia, safe harbor principle is primarily discussed in the context of copyright protection on User-Generated Content (UGC) platforms like social media and in the e-commerce domain (Maulana & Aristi, 2025). Additionally, the concept is implemented within international data privacy frameworks, such as between the United States and the European Union, to legitimize cross-border data transfers. Academics also continue to propose expanding the application of safe harbor to new areas, such as protecting researchers conducting security evaluations on artificial intelligence (AI) systems from lawsuits, and for providers of open, distance, and digital education (ODDE) in Indonesia to protect institutions from potential violations during the online teaching and learning process (Longpre et al., 2024).

Article 26 paragraphs (3) and (4) of Law No. 19 of 2016, which amends the ITE Law, implicitly establish a safe-harbor mechanism by requiring electronic system providers to delete irrelevant information or electronic documents at the request of copyright holders and to provide a mechanism for doing so in accordance with applicable regulations. However, Government Regulation No. 71 of 2019 on the Provision of Electronic Systems and Transactions does not explicitly regulate safe-harbor obligations, instead requiring providers under Article 31 to protect users and the public from potential harm arising from their systems and, under Article 32 paragraph (1), to secure and protect the facilities and infrastructure of their electronic systems. To offer greater legal clarity, the Minister of Communication and Informatics issued Circular Letter No. 5 of 2016 on the Limitations and Responsibilities of Platform Providers and Merchants Through Electronic Content, which outlines the respective obligations and responsibilities of parties involved in e-commerce (Hermawan & Pramana, 2022).

The sale of shared premium accounts for digital platforms must come from a clear source. In the case of selling and buying shared premium platform accounts through third parties on e-commerce, the positive law provisions in Indonesia are violated, where the sale of shared premium accounts should only be done officially on the application's platform, but is now easily obtainable through third parties. Premium account products from third parties are marketed through e-commerce with prices lower than the official platform. In relation to the sale of premium platform accounts by third parties, a previous discussion was conducted in a 2024 study by Latulola et al. (2024)titled "*Legal Protection for Netflix Regarding the Sale of Premium Accounts on Social Media*," which discussed copyright infringement related to the sale of premium Netflix accounts through social media. Additionally, there is a 2025 study by Dewi et al. (2025) titled "*A Juridical Review of the Illegal Sale and Purchase of Netflix Premium Accounts*," which discussed losses to copyright owners and legal consequences, such as copyright and ITE Law violations due to the illegal sale of Netflix accounts.

However, this article is distinct and provides a deeper jurisprudential contribution. It specifically analyzes the comparative regulation of platform (ESP) accountability for facilitating illegal sales on e-commerce, focusing on the conditions under which a platform loses its immunity (liability-triggering conditions). This distinction goes beyond simply discussing copyright infringement or criminal sanctions at the seller level, instead concentrating on platform-specific liability. The study aims to examine the legal frameworks governing the liability of digital platforms in relation to the illegal sale of premium subscription accounts. Furthermore, the article explores the fundamental structural differences between the Indonesian Civil Law and United States Common Law approaches to liability limitation and the specific mechanisms of exculpation. It also seeks to identify the legal and economic impacts of regulatory uncertainty on platform operations (the Chilling Effect) and proposes a novel, specific policy recommendation to strengthen Indonesia's protective framework: the Sui Generis Safe Harbor Model.

B. Method

This research employs a doctrinal legal research method with a descriptive-analytical specification that focuses on a statutory provisions (Raof et al., 2025). The approaches used include the statutory approach, comparative approach, and the conceptual approach (Nugroho et al., 2020). The legal materials consists of primary legal materials, namely relevant laws and regulations from the Republic of Indonesia such as the Job Creation Law (Copyright Cluster) and the ITE Law, as well as the Digital Millennium Copyright Act from the United States (Nur, 2021). Secondary legal materials include books, scientific journals, theses, and other literature that support the research (Febriani & Yulianingsih, 2019).

The legal materials collection technique is conducted systematically through a document study, beginning with the inventory and collection of all primary and secondary legal materials. Subsequently, the collected legal materials are analyzed qualitatively. The legal materials analysis method involves processing and interpreting these legal materials, then constructing logical and systematic legal arguments. The results of this analysis of legal facts are then formulated into writing to draw a logical conclusion that answers the research problem.

The choice to compare with the United States is based on the significance of the Digital Millennium Copyright Act (DMCA) of 1998, which is the most pioneering and comprehensive legal framework globally in regulating the liability of digital platforms (ISPs) regarding user copyright infringement. This comparison is essential to highlight the contrast between the explicit legal framework in the United States and Indonesia's more implicit, fragmented, and less specific approach to adopting the safe harbor principle. The difference is particularly notable given that the US follows Common Law (precedent-based), while Indonesia adheres to Civil Law (codified law), which significantly impacts the implementation of technical standards like Red Flag Knowledge. The heart of this comparison lies in contrasting the US's mechanism-based Notice and Takedown

exoneration criteria with Indonesia's reliance on the general principle of good faith and fault-based liability (Article 15(3) of the ITE Law). This comparative analysis aims to offer concrete recommendations for Indonesia in developing clearer safe harbor regulations.

C. Results and Discussion

1. Regulation of the Selling Shared Premium Digital Platform Accounts on E-Commerce Under United States and Indonesian Law

Several relevant regulations have been established in Indonesia, reflecting the government's role as a primary stakeholder in addressing the issue of illegal premium account sales (Wibowo, 2023). However, none of these regulations specifically define "safe harbor" in the context of digital platforms or clarify how violations related to sharing premium account subscriptions should be handled. Indonesia relies on a combination of existing laws, whose relevant provisions can be interpreted to address this issue. In the case of selling shared premium account services on e-commerce platforms, business actors violate Article 9, Paragraph 3 of Law No. 28 of 2014 concerning Copyright (Copyright Law), which states that "Any person who, without the permission of the creator or copyright holder, is prohibited from duplicating and/or commercially using a creation." This implies that commercial use of a shared premium subscription account infringes upon the creator's exclusive rights (Gumilang & Kristianto, 2025).

These business actors failed to obtain official permission to reproduce or grant access to the shared premium platform account, thereby violating the license agreement. According to Article 113, Paragraph (3) of the Copyright Law, anyone who reproduces and distributes a creation for commercial use without the rights and/or permission from the creator or copyright holder may face a prison sentence of up to four years and/or a fine of up to IDR 1,000,000,000 (one billion rupiah) (Tambunan et al., 2023). The economic rights of the creator and/or copyright holder of the digital platform are harmed by the distribution actions carried out by third-party sellers through e-commerce. As a result, the creator or other affected parties are entitled to seek compensation for these losses through a court ruling (Rukmana & Ramadhita, 2022). The transactions between third-party sellers and customers on e-commerce platforms constitute a violation of good faith and legal provisions based on the Civil Code, the ITE Law, and the Copyright Law. Therefore, such actions are deemed illegal (Yanti, 2023).

The basis for safe harbor is implicitly established by Article 15, Paragraph (3) of the ITE Law, as amended by Law No. 1 of 2024. According to this article, losses arising from the malfunction or disruption of an Electronic System that are not caused by the fault of the Electronic System Provider (ESP) are not the responsibility of the ESP. Protection is granted to the platform if the violation is committed by a user without the knowledge or negligence of the platform, and if the platform has taken reasonable steps to maintain the reliability of its system in accordance with the principle of based on fault. (Revaldi, 2021). Although safe harbor is not directly mentioned, the ITE Law encourages the ESP's responsibility to operate electronic systems securely and reliably. Furthermore, Government Regulation No. 80 of 2019 concerning Trade Through Electronic Systems, signed by President Jokowi, stipulates the obligation for Providers of Trade Through Electronic Systems to make efforts to prevent the misuse of their systems (Tampubolon et al., 2020). For example, a Providers of Trade Through Electronic Systems is required to ensure the legality of goods/services in accordance with Article 13, and mechanisms for handling complaints and blocking illegal content are regulated in Articles 48 and 53.

Article 45 of Government Regulation No. 71 of 2019 concerning the Provision of Electronic Systems and Transactions further emphasizes the legal obligations of parties engaging in electronic transactions. It states that parties involved in such transactions will face legal consequences if they fail to comply with the regulations. The regulation also outlines several key principles that must guide the implementation of electronic transactions. These include fairness, which ensures that all

parties are treated equitably; prudence, emphasizing the need for careful and responsible decision-making; good faith, which requires honesty and integrity in transactions; accountability, ensuring that parties are responsible for their actions; and transparency, which calls for openness and clarity in the transaction process. These principles are intended to foster a secure, ethical, and trustworthy digital environment, where electronic transactions are conducted in a manner that protects the rights of all parties involved and ensures compliance with the law (Zaklylen, 2025)

Additionally, Law No. 8 of 1999 concerning Consumer Protection (Consumer Protection Law) plays a crucial role in ensuring that digital platforms are responsible for the integrity of their subscription services. If a license violation for a shared premium account occurs on a platform due to negligence or deliberate inaction, it can be seen as a violation of the principle of good faith (Article 7 Consumer Protection Law) (Jusar et al., 2023). The rights of consumers who have paid for legitimate access can be harmed because accounts that are proven to violate terms are not blocked, illegal account sellers are not acted against, or adequate security systems to prevent unauthorized account sharing are not implemented in the platform's terms. Consumers who feel aggrieved by the platform's negligence or inaction regarding license violations can file a complaint under the Consumer Protection Law. Platforms must ensure the integrity of their services from the sale of illegal products/services and that the rights of legitimate subscribers are not violated by the actions of irresponsible third parties (Ponow, 2025).

Based on the explanation above regarding the positive law regulations in Indonesia that govern safe harbor in the context of digital platforms and premium account license violations, it is evident that these regulations remain implicit. Premium account license violations indirectly breach the Copyright Law by commercially using a work without the creator’s permission. However, this violation is not explicitly addressed in the context of the digital business model on platforms, particularly concerning the illegal resale of shared premium accounts on e-commerce sites. The primary issue lies in the fragmentation of laws and the absence of a clear mechanism for platforms to proactively limit liability, which is crucial for an effective safe harbor regime.

A key challenge arises from the structural differences between Indonesia’s Civil Law system, which is based on codified, broad principles such as good faith, and the US Common Law system, which relies on precedent and precise judicial interpretation. This divergence significantly limits Indonesia's ability to implement detailed and technical safe harbor standards, making it more difficult to provide clear guidelines for digital platforms. As a result, while Indonesia has made progress in regulating digital platforms, the lack of specific provisions for safe harbor complicates the enforcement of liability limitations and hampers the development of a comprehensive regulatory framework for the digital economy.

This research will compare the regulations concerning safe harbor in the context of digital platforms and premium account license violations in Indonesia with the regulations in the United States. In the United States, the Digital Millennium Copyright Act (DMCA), enacted in 1998, is a pioneer in regulating the liability of internet service providers (ISPs) or digital platforms regarding copyright infringement committed by their users (Ponow, 2025). The purpose of the DMCA is to ensure that the interests of copyright owners are not violated and to introduce legal protections (safe harbors) for ISPs or digital service/platform providers from liability for copyright infringements committed by their users (Prihatin et al., 2024). This protection is regulated in Section 512 of the DMCA. To qualify for safe harbor protection, an ISP must meet several general and specific criteria depending on the type of service they provide.

Section 512 of the Digital Millennium Copyright Act (DMCA) outlines four key categories of Safe Harbor protection designed to shield online service providers (ISPs) from liability for copyright infringement committed by their users (Davies, 2020). The first category, Transitory Digital Network Communications (Section 512(a)), offers protection to ISPs for the temporary transmission of data across their network. This includes activities such as automatic routing and caching, where the service provider does not actively control or modify the content being

transmitted. Essentially, this provision ensures that ISPs are not held responsible for fleeting instances where content simply passes through their infrastructure without being stored or altered, safeguarding their role as intermediaries in the digital ecosystem.

The second category, System Caching (Section 512(b)), extends the Safe Harbor protections to ISPs for the automatic and temporary storage of content copied from other websites or online sources to enhance network efficiency. This process, known as caching, occurs when data is stored temporarily on a network to reduce delays for subsequent requests. As long as the ISP follows the requirements of this provision, such as ensuring that cached content is not modified and is promptly deleted when no longer needed, the ISP is shielded from liability for infringement. This protection is crucial for maintaining the efficiency and performance of the internet, allowing for faster content delivery without placing undue burden on service providers.

The third and most relevant category is Information Residing on Systems or Networks at the Direction of Users (Section 512(c)), which applies to user-generated content (UGC) platforms, such as YouTube, Facebook, or e-commerce sites that host user-uploaded content. This provision offers the most extensive protection for ISPs, provided they meet certain conditions. First, the ISP must not have actual knowledge of the infringing activity. If the ISP becomes aware of infringing content, either through actual knowledge or through a "Red Flag" standard that indicates infringement, the provider must act promptly to remove or disable access to the infringing material. Additionally, the ISP is protected only if they do not receive a direct financial benefit from the infringing activity. In other words, platforms that directly profit from the unlawful content, such as through advertising revenue linked to that content, may lose their Safe Harbor protection. The notice-and-takedown procedure is integral to this provision: once the ISP is notified of the infringement, they must take swift action to address the issue, often by removing or disabling access to the infringing content. This process aims to balance the protection of copyright holders with the operational realities of managing massive platforms where user-generated content is prevalent.

Finally, Information Location Tools (Section 512(d)) protects providers of tools such as search engines or hyperlink services, which direct users to content hosted elsewhere on the internet. These tools, while facilitating access to content, do not host or store the content themselves. Section 512(d) ensures that these providers are not held liable for copyright infringements related to the content they link to, as long as they do not play a direct role in storing or serving that content. This Safe Harbor provision protects services that make it easier for users to find relevant information, such as search engines or content aggregation platforms, from being held accountable for the infringing activities of third-party websites they link to.

This research focuses more on the safe harbor in Section 512(c) regarding the notice and takedown mechanism. When a copyright owner finds material that infringes their copyright on an online platform, they can send a valid takedown notice to the platform (Nwabachili & Udeoji, 2021). After a valid takedown notice is received, access to the reported material must be promptly removed or disabled by the platform. If the platform fails to act quickly, it loses its safe harbor protection and can be held liable for the infringement. Although safe harbor provides significant protection, there are limitations that prevent platforms from abusing this protection, namely the concepts of Red Flag Knowledge and the right and ability to control. The concept of Red Flag Knowledge means the platform has knowledge of facts or circumstances that objectively indicate the presence of clear and obvious infringing activity (Samuelson, 2020). An example would be a video title that is clearly a copyright violation, such as “Full Movie: Pirated Film X.” The concept of Right and Ability to Control means that if a platform not only stores content but also actively encourages, induces, or receives a direct financial benefit from the infringing activity, it may lose its safe harbor (Frosio & Geiger, 2023).

A case study on platform liability is *Viacom v. YouTube*, a case concerning illegal streaming. Viacom, a major copyright owner including MTV and Comedy Central, sued YouTube for

massive copyright infringement, claiming that YouTube passively benefited from millions of user-uploaded videos without permission (Rafli, 2024). Viacom argued that YouTube had Red Flag Knowledge and the right and ability to control the infringing material on their platform. YouTube argued that they were protected by the DMCA safe harbor because they were a service provider storing user-uploaded content and they acted quickly to remove content after receiving a valid takedown notice. The *Viacom v. YouTube* case showed that YouTube was protected by the DMCA safe harbor, with a federal appellate court ruling emphasizing that Red Flag Knowledge must be actual knowledge of specific infringements, not merely general knowledge of the existence of infringing content (Gesmer, 2025). The court also ruled that YouTube did not actively encourage infringement. This ruling became a significant precedent, strengthening safe harbor protection for UGC platforms in the United States and affirming the role of the notice and takedown mechanism. As a result, platforms like YouTube were encouraged to invest in technology such as Content ID to make it easier for copyright owners to identify and manage their content, reducing the need for manual takedown notices (Pratama, 2017b).

This specific judicial interpretation is the key difference, illustrating how the United States system provides clear judicial guidance on when immunity is *lost* based on explicit knowledge and control requirements.This differs from the legal framework in Indonesia, where the burden of proof is less focused on the platform's subjective knowledge of specific infringing activity. The comparative analysis reveals that Indonesia's implicit framework relies on the general principle of liability based on fault (Article 15(3) ITE Law), coupled with the concept of awareness of facts or circumstances that leads to knowledge (Government Regulations 80/2019), which serves as the implicit equivalent of the DMCA's Red Flag Knowledge. However, this lack of codified procedural specificity particularly the absence of a standardized notice and takedown mechanism makes Indonesian platforms inherently more vulnerable to litigation and legal uncertainty compared to their US counterparts operating under explicit, precedent-defined conditional protection.

Table 1.
Comparison of Regulations on the Sale of Shared Premium Accounts on Digital Platforms: Indonesia Vs. United States

Aspect	Indonesian Law	United States Law
Primary Legal Basis	1. Law No. 28 of 2014 concerning Copyright; 2. Law Number 11 of 2008 concerning Information and Electronic Transactions (ITE Law) as amended by Law Number 1 of 2024; 3. Law No. 8 of 1999 concerning Consumer Protection; 4. Government Regulation Number 71 of 2019 concerning the Provision of Electronic Systems and Transactions; 5. Government Regulation Number 80 of 2019 concerning Trade Through Electronic Systems.	Digital Millennium Copyright Act (DMCA) of 1998, specifically Section 512.
Legal System Structure	Civil Law: Principles are codified in statutes, relying on broad interpretation of good faith and negligence.	Common Law: Principles developed by judicial precedent (casuistic), providing highly technical standards (e.g., *Viacom v. YouTube*).
Platform Liability	Not explicitly defined, but implicitly protects platforms from liability if certain procedures are followed, and the protection is less strict. It relies on the	Strict and explicit protection; platforms must follow the "notice and takedown" procedure to obtain "safe harbor." Protection is conditional on compliance with specific knowledge and control requirements (e.g.,

Aspect	Indonesian Law	United States Law
	principle of *good faith* and *liability based on fault* (Article 15(3) ITE Law).	Red Flag Knowledge and Right/Ability to Control).
Equivalent Knowledge Element	Implicit: awareness of facts or circumstances that leads to knowledge (Government regulations 80/2019).	Explicit: Red Flag Knowledge (facts or circumstances from which infringing activity is apparent), defined by clear judicial precedent.
Weakness	Protection is merely implicit, not specific or clear, leading to potential legal uncertainty in its implementation. The lack of a standardized *Notice and Takedown* mechanism places a higher, less measurable burden on platforms.	Requires strict compliance with specific procedures. Conceptually, platforms must be able to prove they had no direct knowledge of and did not actively encourage the infringement. However, judicial precedents (e.g., *Viacom v. YouTube*) provide crucial clarity on the definition of knowledge and control.

Source: Author's Compilation (2025)

Although Indonesian laws implicitly provide room for limiting the liability of Electronic System Providers (ESP), as seen in Article 15 Paragraph (3) of the ITE Law and related regulations under the Government Regulation on Trading Through Electronic Systems, the legal protection afforded to ESPs in Indonesia is relatively weaker and more prone to legal uncertainty when compared to the United States. The safe harbor provisions in Indonesia, while present, do not offer the same level of certainty and security for ESPs, which can discourage innovation and growth in the digital ecosystem. This vulnerability stems from several key factors that contribute to the frailty of the current legal framework. Firstly, there is a notable absence of an explicit and standardized notice-and-takedown mechanism in Indonesian law. In contrast to the United States, where the Digital Millennium Copyright Act (DMCA) provides a clear and detailed process for removing infringing content, Indonesian law lacks such a well-defined process, leaving ESPs with uncertainty about their obligations and potential liabilities.

Secondly, the legal framework in Indonesia heavily relies on a broad interpretation of the principle of good faith and bases liability on fault. This reliance on subjective judgment opens up room for interpretation, leaving platforms in a precarious situation. In practice, the determination of whether an ESP is liable for user-generated content often hinges on internal factors such as the effectiveness of the platform's violation reporting system, the integrity of the data or evidence related to the violations, and the platform's response in managing such violations. However, these factors are not explicitly regulated in the law, creating inconsistency in how platforms are treated across different cases. Without clear, uniform guidelines on how to handle complaints and takedown requests, ESPs in Indonesia face the risk of being held accountable for content over which they may not have direct control, particularly in the absence of a robust and transparent system for reporting and addressing illegal or harmful activities.

Moreover, the lack of a standardized takedown process makes it difficult for ESPs to implement consistent procedures to mitigate risks. Unlike in the United States, where platforms can rely on the DMCA's clear protocols for addressing infringing content, Indonesian platforms must navigate the complexities of a vague legal framework, where the response to violations is often discretionary and subjective. This results in a situation where platforms may be exposed to legal challenges without adequate protection, particularly when content is flagged but not removed in a timely or transparent manner.

Ultimately, this absence of clear and measurable protective mechanisms puts platforms in Indonesia at a significant disadvantage compared to their counterparts in countries like the United States, where the legal environment provides more certainty and security through well-established laws. In Indonesia, the lack of explicit guidelines leaves ESPs more vulnerable to lawsuits, potentially stifling innovation and discouraging investment in the digital ecosystem. The uncertainty surrounding liability and the insufficient legal protections can create an environment

where platforms are reluctant to take risks or expand their services, limiting the potential growth and development of Indonesia's digital economy. Therefore, strengthening the legal framework with clearer, more standardized procedures for liability and takedown mechanisms is crucial to fostering a more secure and innovative digital environment in Indonesia.

2. Impacts of Illegal Premium Account Subscription License Violations for the Parties Involved

Premium account subscription license violations have far-reaching consequences that affect the entire digital ecosystem, including platforms, e-commerce sites, and the broader market. For digital platforms, the economic impact is significant. The illegal sale of premium accounts directly diminishes revenue from legitimate subscriptions, which is crucial for sustaining the platform's financial health. This loss of income can hinder investment in innovation, content production, and platform improvement. Additionally, platforms risk damage to their reputation when illegal accounts are involved. These unauthorized accounts are often of lower quality or display intrusive advertisements, which tarnishes the platform's image and undermines the trust it has built with customers. Such violations can also hurt the service provider's standing, especially when the business practices sound ethics and aims to maintain a positive brand image. The practice of reselling illegal accounts undermines the subscription-based business model that forms the backbone of many digital platforms. As a result, these platforms face direct financial losses and a long-term decline in consumer trust, both of which can limit their capacity to thrive in a competitive market (Yohanis et.al, 2020).

E-commerce sites that facilitate the sale of illegal premium accounts also face considerable risks due to the ambiguity surrounding the safe harbor principle. The lack of clear legal guidelines for platforms, specifically the absence of a well-defined 'Red Flag Knowledge' standard, exposes e-commerce platforms to significant legal risk. This ambiguity creates what is known as the "Chilling Effect," where platforms are unsure of their legal obligations and may avoid taking action out of fear of potential lawsuits (Samuelson, 2021). Specifically, the absence of a clearly codified 'Red Flag Knowledge' standard, exposes platforms to lawsuits based on vague notions of 'negligence' or failure to act in 'good faith'. The absence of a clearly codified framework leaves platforms vulnerable to legal challenges based on vague interpretations of 'negligence' or failure to act in 'good faith.' If platforms do not fulfill their takedown obligations or are deemed negligent in preventing the sale of illegal accounts, they may face excessive lawsuits from copyright holders. The legal and operational burden of handling these cases is immense, as platforms must navigate non-standardized infringement reports and determine appropriate actions on a case-by-case basis. This unpredictability increases litigation costs and diverts technological resources away from development, ultimately stifling innovation and deterring potential investment in the creation of new digital platforms. Without a clear and enforceable safe harbor standard, the digital ecosystem remains hindered, unable to reach its full potential in fostering innovation and sustainable growth (Rahman, 2022).

The process of identifying, verifying, and removing illegal listings on digital platforms creates a significant operational burden for the platforms involved. This burden is not only costly but also resource-intensive, requiring platforms to implement rigorous systems to monitor and manage potentially illegal activities. For sellers of illegal accounts, the consequences are severe. They face both criminal and civil sanctions under existing copyright laws. As outlined in this paper, sellers of illegal accounts can be sentenced to imprisonment of up to four years and/or face fines of up to IDR 1 billion. Furthermore, economic damages can be claimed from these sellers, providing an additional deterrent. These legal provisions underscore the serious nature of account license violations and the importance of upholding intellectual property rights in the digital space.

Buyers of illegal accounts also face numerous risks and potential losses. Financially, they are exposed to the possibility of losing the value of their purchase, as the account can be blocked by

the legitimate service provider without any refund. In addition, purchasing accounts from unauthorized third-party sellers exposes buyers to data security risks. Accounts obtained through these channels are often insecure, making them vulnerable to personal data theft, fraud, or other forms of cybercrime. The lack of guarantee regarding continued access to the service is another significant risk. Buyers may find that their access to the service is cut off at any time, often without prior warning, leaving them with no recourse for recovery. This combination of financial loss, data security threats, and unreliable access underscores the importance of enforcing legal frameworks that protect both consumers and service providers in the digital economy.

3. Recommendations Regarding Illegal Premium Account Subscription License Violations for the Parties Involved

The comparative findings highlight the need for Indonesia to go beyond relying solely on the ITE Law and to develop a specific (sui generis) legal regime for robust digital copyright protection. This new framework should combine the legal certainty of the DMCA's procedural approach with Indonesia's Civil Law tradition. The objective is to create a system that provides clearer guidelines for digital platforms while considering Indonesia's unique legal context. By adopting such a model, Indonesia can better address the complexities of digital copyright infringement and offer more effective protection for creators, consumers, and platforms.

In terms of legislative recommendations, several key amendments to the relevant legal regulations are necessary. First, it is essential to explicitly define digital license violations and the concept of safe harbor in the law, providing legal clarity and a stronger foundation for enforcement. Clear definitions will help prevent ambiguity and ensure that platforms and users understand their rights and obligations. Additionally, establishing clear and measurable due diligence standards for e-commerce platforms is crucial. These standards should include specific guidance on the steps platforms must take to prevent violations, such as seller verification, illegal content detection, and timely responses to infringement reports. Lastly, the harmonization of regulations across relevant sectors—such as Intellectual Property, Information Technology, and Trade—will create a more cohesive legal framework. This approach will help avoid the loopholes or overlaps that often occur when different regulations are applied separately, ultimately ensuring a more effective and efficient regulatory environment.

The Sui Generis Model in Indonesia for regulating digital platforms aims to create a stronger legal framework that enhances accountability and protection for Electronic System Providers (ESPs) while fostering a safer digital ecosystem. To achieve this, several key components need to be incorporated into the model to address existing gaps in the current regulatory system.

One key component that should be included is the Codified Red Flag Standard, specifically designed for digital subscription products. This standard would provide clear, measurable, and objective criteria to identify illegal or harmful activities on platforms. ESPs would be required to implement mandatory due diligence procedures, and their immunity from liability would be revoked if they are found to be hosting listings that contain certain red flags. These red flags might include prohibited keywords such as “shared account” or “lifetime access for monthly service,” which are often associated with fraud or intellectual property violations. Additionally, listings with unreasonably low pricing, such as offering products at 50% below the official retail price, would raise concerns as such pricing often signals unauthorized sales or illegal activities. The model would also address mass listing patterns by a single seller, which could indicate suspicious behavior such as the mass distribution of pirated digital products. By codifying these red flag criteria, the Sui Generis Model would provide a clear legal framework for platforms to follow, reducing ambiguity and enhancing their ability to prevent illegal activities.

Another essential element of the Sui Generis Model is the introduction of a mandatory Notice and Takedown procedure. This procedure would require legislation to establish a formal, centralized, and standardized process that obligates platforms to act quickly upon receiving a valid

infringement notice. For example, platforms would need to remove infringing content within 24 to 48 hours of receiving a notice. This approach ensures that platforms are proactive in responding to intellectual property violations, reducing the potential for legal disputes. Moreover, it provides a clear and consistent process for content creators and other stakeholders to address their complaints. By formalizing this procedure, the model would help reduce the uncertainty that currently surrounds content takedowns, fostering a more transparent and trustworthy digital marketplace.

Lastly, the Sui Generis Model should introduce a data disclosure condition as part of the safe harbor protection for platforms. Under this condition, platforms would only retain immunity from liability if they comply with requests to provide subscriber information to law enforcement and regulatory bodies for supervision and enforcement purposes. This would ensure that platforms are not only acting in the best interest of their users but also supporting efforts to maintain a lawful and ethical digital environment. By mandating data disclosure in certain circumstances, the model would promote greater accountability and allow authorities to address illegal activities more effectively, without infringing on users' privacy rights.

From a policy perspective, increased coordination among key law enforcement agencies such as Kominfo, the National Police, and the Directorate General of Intellectual Property is crucial. Given that handling license violation cases often involves multiple jurisdictions, effective coordination between these agencies will ensure better enforcement and more consistent legal action. In addition, public education campaigns focused on the legality of digital transactions and the risks of engaging in illegal practices need to be significantly strengthened. Many consumers, as well as sellers, may not fully comprehend the legal consequences and the potential risks associated with these illegal activities. Raising awareness through targeted campaigns can help bridge this gap and reduce the prevalence of such practices.

Moreover, the development of best practice guidelines for e-commerce platforms, through collaboration between the government and industry stakeholders, will be essential. These guidelines would assist platforms in implementing preventive and enforcement measures that are both effective and legally sound. By creating clear, shared standards for e-commerce operations, platforms can more easily navigate legal requirements and avoid unknowingly facilitating illegal activities.

From a technical and operational standpoint, e-commerce platforms must adopt more advanced detection technologies, such as artificial intelligence (AI), to identify illegal product listings. Platforms should invest in AI systems capable of automatically detecting and blocking attempts to sell illegal accounts or engage in account-sharing practices that violate platform terms. These technologies would help streamline the process of identifying and removing infringing content before it reaches a wider audience, ultimately protecting both consumers and rights holders.

In addition, platforms should implement stricter onboarding processes for sellers of digital products. This should include comprehensive identity verification procedures and checks to ensure the legality of the goods or services being sold. By verifying sellers upfront, platforms can reduce the likelihood of unauthorized products being sold and make it harder for bad actors to exploit the platform. A robust onboarding system would also build trust with consumers, who are increasingly looking for secure and verified sources for their digital purchases.

Furthermore, an effective and responsive violation reporting mechanism is essential for ensuring that illegal activities are swiftly addressed. Platforms must ensure that there is a clear and easily accessible system for users to report potential violations. Once a report is received, the platform should have a transparent process in place to investigate and take appropriate action within a short time frame. This ensures that users feel empowered to report suspicious activities and that platforms respond promptly to mitigate potential harm.

For the service provider platforms themselves, there are two main recommendations. First, platforms should continue to innovate and develop security features and technologies aimed at detecting and preventing unauthorized account-sharing practices. As digital landscapes evolve, so do the methods employed by bad actors, making it essential for platforms to stay ahead with proactive security measures. Second, platforms must take a more active role in monitoring and reporting violations. Copyright holders and platforms cannot simply wait for violations to occur; they need to monitor e-commerce and other digital platforms consistently, identifying and reporting illegal listings as quickly as possible. By doing so, they contribute to a more secure digital environment and help ensure that violators face timely consequences.

D. Conclusion

The rapid expansion of Indonesia's digital economy—driven in large part by subscription models and platforms offering premium services such as Netflix and Spotify—presents substantial opportunities for growth and innovation. At the same time, the illegal resale and sharing of premium accounts on e-commerce platforms has introduced acute legal, economic, and reputational risks for platforms, sellers, and consumers alike. Indonesia currently faces a regulatory gap: the safe-harbor principle and legal protections for license violations are largely implied rather than explicitly defined, leaving Electronic System Providers (ESPs) exposed to legal uncertainty. Unlike the United States, which has the DMCA and a well-developed notice-and-takedown regime clarified by case law on the meaning of "knowledge," Indonesia needs more precise and comprehensive statutory guidance to address these cross-cutting challenges effectively.

Practically, account-sharing and unauthorized sales undermine platform revenue, erode consumer trust, and create long-term threats to sustainable business models while complicating enforcement of consumer protection and intellectual property rights. To reduce legal ambiguity and strengthen enforcement, Indonesia should pursue coordinated regulatory revision and policy harmonization that clearly delineates ESP obligations, tightens safe-harbor criteria, and sets out predictable remedies for rights holders. Enhanced interagency coordination—among Kominfo, the National Police, and the Directorate General of Intellectual Property—is essential because many infringement cases cross jurisdictional and sectoral boundaries; clearer institutional roles will reduce enforcement gaps. Parallel public education campaigns are also vital to warn consumers and sellers about the legal risks and harms of participating in or facilitating the illicit market for shared accounts.

On the technological and operational fronts, platforms must invest in advanced detection and prevention tools—particularly AI-driven systems that can identify fraudulent listings and patterns of unauthorized account sharing—and adopt stricter seller onboarding practices including identity verification and provenance checks for digital goods. Robust, transparent reporting and takedown mechanisms will allow platforms to act swiftly when violations occur, and a proactive monitoring stance (rather than waiting solely for third-party notices) will better protect ecosystems from abuse. Together, these regulatory, institutional, technical, and educational measures can create a safer, fairer digital environment in Indonesia—one that preserves consumer rights, protects intellectual property, and supports a resilient digital economy in which all stakeholders are accountable.

REFERENCES

Abduh, R., & Fajaruddin. (2021). Intellectual Property Rights Protection Function in Resolving Copyright Disputes. *IJRS: International Journal Reglement& Society*, *2*(3), 170–178. https://doi.org/https://doi.org/10.55357/ijrs.v2i3.154

Achya, S. H. F., Yuliana, Tri, I., & Pangesti, N. (2023). Perlindungan Hukum Terhadap Pengguna

Layanan Aplikasi Premium yang Diperoleh dari Pihak Ketiga. *Diponegoro Private Law Review*, *10*(2), 198–222. https://ejournal2.undip.ac.id/index.php/dplr/article/view/18946

Avirutha, A. (2021). ASEAN in Digital Economy : Opportunities and Challenges. *Journal of ASEAN PLUS+ Studies*, *2*(1), 17–25. https://so06.tci-thaijo.org/index.php/aseanplus/article/view/245334

Cahyono, D. N., Putri, K., Afkarina, I., Aprilia, P., & Jember, S. (2023). Bangkitnya Perekonomian Indonesia Pasca Covid-19. *Jurnal Ekonomi Bisnis Dan Kewirausahaan*, *12*(1), 59–75. https://doi.org/https://doi.org/10.47942/iab.v12i1.1327

Davies, R. E. (2020). Ebb and Flow in Safe Harbors : Some Exemplary Experiences Under One Old Statute and One New. *Center for the Protection of Intellectual Property, Policy Briefs & Issue Papers*, *September*. https://cip2.gmu.edu/wp-content/uploads/sites/31/2020/09/Davies-Ebb-and-Flow-in-Safe-Harbors.pdf

Dewi, N. M. T. A., Budiartha, I. N. P., & Ujianti, N. M. P. (2025). Tinjauan Yuridis Terhadap Layanan Jual Beli Account Netflix Premium Secara Ilegal. *Jurnal Analogi Hukum*, *7*(1), 94–99.

Ekawijaya, A. B., Rahayu, A., & Dirgantari, P. D. (2023). Strategi Penetapan Harga Layanan Education Technology (Edtech) Indonesia. *Jurnal Ilmu Manajemen Dan Bisnis*, *14*(1), 87–98. https://doi.org/10.17509/jimb.v14i1.57003

Febriani, R. F., & Yulianingsih, W. (2019). Implementasi Asas Keseimbangan Dalam Transaksi Jual Beli Di Giyomi ID Online Shop. *Simposium Hukum Indonesia*, *1*(1), 379–384. https://journal.trunojoyo.ac.id/shi/article/view/6351

Frosio, G., & Geiger, C. (2023). Taking fundamental rights seriously in the Digital Services Act's platform liability regime. *European Law Journal*, *29*(1–2), 31–77. https://doi.org/10.1111/eulj.12475

Gesmer, L. (2025). *Second Circuit Revisits DMCA "Red Flag" Safe Harbor, Building on Youtube Legacy*. https://www.masslawblog.com/dmcacda/second-circuit-revisits-dmca-safe-harbor-building-on-youtube-legacy/

Gumilang, N. P., & Kristianto, F. (2025). Legal Protection of Copyright Towards Work Piracy for ' Paid Stories ' Written Works on Wattpad Platform : A Case Study in Indonesia. *European Journal of Law and Political Science*, *4*(2), 15–21. https://doi.org/10.24018/ejpolitics.2025.4.2.168

Hermawan, A. W., & Pramana, Y. (2022). Secondary Liability and Safe Harbors for Platform Providers in Indonesian E-Commerce Law. *Scientium Law Review (SLR)*, *1*(3), 101–108. https://doi.org/10.56282/slr.v1i3.335

Hildawati, H., Haryani, H., Umar, N., Suprayitno, D., & ... (2024). *Literasi Digital: Membangun Wawasan Cerdas dalam Era Digital terkini* (Issue April). PT. Green Pustaka Indonesia.

Junaedi, D., Supriyatna, R. K., Arsyad, M. R., & Amalia, R. S. (2022). Peluang dan Ancaman Disruptif Digital untuk Negara Berkembang. *Sci-Tech Journal*, *2*(2), 120–141. https://doi.org/10.56709/stj.v2i2.71

Jusar, R., Taher, P., & Dwivismiar, I. (2023). Tanggungjawab Pelaku Usaha dan Marketplace terhadap Pelanggaran Asas Itikad Baik dalam Transaksi E-commerce. *Sultan Jurisprudence: Jurnal Riset Ilmu Hukum*, *3*(1), 62-72. https://doi.org/10.51825/sjp.v3i1.19234

Latulola, V. A., Kuahaty, S. S., & Pesulima, T. L. (2024). Perlindungan Hukum Netflix Atas Penjualan Akun Premium Di Media Sosial. *PATTIMURA Legal Journal*, *3*(1), 45–55. https://doi.org/10.47268/pela.v3i1.13261

Longpre, S., Kapoor, S., Klyman, K., Ramaswami, A., Bommasani, R., Blili-Hamelin, B., Huang, Y., Skowron, A., Yong, Z. X., Kotha, S., Zeng, Y., Shi, W., Yang, X., Robey, R. S. A., Chao, P., Yang, D., Jia, R., Kang, D., Pentland, S., … Henderson, P. (2024). Position: A Safe Harbor for AI Evaluation and Red Teaming. *Proceedings of Machine Learning Research*, *235*, 32691–32710. https://doi.org/10.48550/arXiv.2403.04893

Maulana, M. A., & Aristi, S. (2025). Copyright Ownership of News Content on User Generated Content Based Platforms in Kompasiana. *Arena Hukum*, *18*(1), 32–52. https://doi.org/https://doi.org/10.21776/ub.arenahukum2025.01801.

Meidyasari, S. (2024). The Impact of Digital Economy in Driving Economic Growth and Development in Indonesia. *INJURITY: Journal of Interdisciplinary Studies*, *3*(11), 777–783. https://doi.org/https://doi.org/10.58631/injurity.v3i11.1306

Nugroho, S. S., Haryani, A. T., & Farkhani. (2020). Metodologi Riset Hukum. In *ase Pustaka* (Vol. 2). (Cetakan Pertama). Oase Pustaka.

Nur, D. S. (2021). *Buku Pengantar Penelitian Hukum*. CV. Penerbit Qiara Media.

Nurullayev, S. S. (2023). Environmental Legal Liability in the Construction Field. *International Journal of Law and Criminology*, *3*(12), 59–66. https://doi.org/10.37547/ijlc/Volume03Issue12-11

Nwabachili, C. C., & Udeoji, N. N. (2021). Copyright Industry And Response To Digital And Online Infringement: UK And USA Experience. *Chukwuemeka Odumegwu Ojukwu University Journal of Commercial and Property Law Journal (COOUJCPL)*, *3*(1), 64–90. https://www.nigerianjournalsonline.com/index.php/COOUJCPL/article/view/2022/0

Ortega, S. (2023). The Digital Millennium Copyright Act – In Need of a Major Software Update. *Michigan Business & Entrepreneurial Law Review,* 12 (1), 75-106. https://doi.org/10.36639/mbelr.12.1.digital

Parmadi, B. D. (2024). Cyber Safe Harbor 4.0: Advancing Ethics and Professionalism in Indonesia's Digital Land-Scape. *Eduvest -Journal of Universal Studies*, *56*(1), 1–54. https://doi.org/10.7560/IC56103.

Ponow, K. S. et. a. (2025). Penegakan Hukum Terhadap Pelaku Usaha yang Menjual Ponsel Ilegal Pada E-Commerce Shopee. *Lex Privatum*, *14*(5), 1–12. https://ejournal.unsrat.ac.id/v3/index.php/lexprivatum/article/view/60261

Pratama, B. (2017a). *Mengenal Safe Harbor Dalam Hukum Siber Indonesia*. https://business-law.binus.ac.id/2017/04/30/mengenal-safe-harbor-dalam-hukum-siber-indonesia/.

Pratama, B. (2017.). *Perspektif Hukum Siber Dalam Menangkap Fenomena Disruptive Innovation*. Seminar Nasional Disruptive Innovation: Kajian Ekonomi dan Hukum, Yogyakarta. https://law.uii.ac.id/wp-content/uploads/2017/07/2017-07-27-fh-uii-semnas-perspektif-hukum-siber-dalam-menangkap-fenomena-disruptive-innovation-bambang-pratama.pdf

Prihatin, L., Listyowati, M. Y. E., & Hidayat, T. I. (2024). Perlindungan Hak Kekayaan Intelektual: Sebuah Esensial Hak Cipta Pada Era Revolusi Industri 4.0. *Unes Law Review, 6*(4), 11321–11329. https://doi.org/10.31933/unesrev.v6i4

Purba, D. S., Dwi Permatasari, P., Tanjung, N., Rahayu, P., Fitriani, R., Wulandari, S., Universitas,), Negeri, I., Utara, S., Muslim, U., & Al Washliyah, N. (2025). Analisis Perkembangan Ekonomi Digital Dalam Meningkatkan Pertumbuhan Ekonomi Di Indonesia. *Jurnal Masharif Al-Syariah: Jurnal Ekonomi Dan Perbankan Syariah*, *10*(1), 126–139. https://doi.org/10.30651/jms.v10i1.25367

Rafli, Z. (2024). Examining Legal Precedents and Social Implications - Interplay Between Intellectual Property Rights and Digital Piracy in the Age of DMCA. *Moccasin Journal De Public Perspective 1*(1), 6–15. 10.37899/mjdpp.v1i1.21

Rahman, N. A. (2022). *Urgensi Pengaturan Praktik Ilegal Lintas Batas Perdagangan Elektronik Terhadap Barang terlarang dan/atau Terbatas*. UIN Syarif Hidayatullah Jakarta.

Ramadhanty, S., Amatullah, N., Setyadani, N. A., & Ramli, T. S. (2020). Doktrin Safe Harbor: Upaya Perlindungan Hak Cipta Konten Dalam Platform User Generated Content. *Legalitas: Jurnal Hukum*, *12*(2), 267-274. https://doi.org/10.33087/legalitas.v12i2.226

Raof, N. A., Aziz, N. A., Omar, N., Othman, R., & Salleh, H. M. (2025). Exploring the Depths : A Comparative Analysis of Doctrinal and Non-Doctrinal Legal Research. *International Journal of Research in Social Science and Humanities (IJRSS)*, *6*(5), 122–129. https://doi.org/10.47505/IJRSS.2025.5.13

Retno Ayu Puspita S, Ramlawati, & Serlin Serang. (2024). Analisis Model Bisnis dan Manajemen Operasional Perusahaan Start-up E-Commerce. *El-Mal: Jurnal Kajian Ekonomi & Bisnis Islam*, *5*(12), 5954–5963. https://doi.org/10.47467/elmal.v5i12.6450

Revaldi, R. (2021). *Tinjauan Hukum Islam Terhadap Perlindungan Hukum Atas Iklan Clickbait di E-Commerce Shopee*. UIN Syarif Hidayatullah Jakarta.

Rukmana, F. I., & Ramadhita. (2022). Pemahaman Hukum Masyarakat Terhadap Pembelian Akun Premium Netflix Tanpa Hak Komersil. *Journal of Islamic Business Law*, *6*(1), 1–11. https://urj.uin-malang.ac.id/index.php/jibl/article/view/1441

Salsabila, N., Rizki, F., Hukum, F., & Udayana, U. (2025). *Jual-Beli Akun Over the Top : Perspektif Hak Cipta (Studi Kasus Pada Penjualan Akun Netflix Secara Ilegal)*. *13*(04), 601–610. https://doi.org/10.24843/KS.2025.v13.i04.p10

Samuelson, P. (2020). Copyright's Online Service Providers Safe Harbors Under Siege. *Communications of the ACM*, *63*(11), 25–27. https://doi.org/10.1145/3423995

Samuelson, P. (2021). Pushing Back on Stricter Copyright ISP Liability Rules. *Michigan Technology Law Review 27* (2), 299-343. https://doi.org/10.36645/mtlr.27.2.pushing

Sawitri, D. A. D., & Dharmawan, N. K. S (2021). Perlindungan Keberadaan Konten Karya Intelektual Dalam Transaksi E-Commerce Berbasis Perjanjian Lisensi. *Kertha Patrika*, *43*(1), 50-64. https://doi.org/10.24843/kp.2021.v43.i01.p04

Setiawan, Z., Dahlan, U. A., & Abdullah, A. (2023). *Konsep Dasar E-Business*. PT Global Eksekutif Teknologi.

Syafrianita, N., Muhammad, A., & Firah, A. (2022). Analisis Perilaku Konsumen Dalam Keputusan Pembelian Produk Pada CV. Syabani di Pusat Pasar Medan. *Jurnal Bisnis Corporate*, *7*(2), 31–40. https://doi.org/10.46576/jbc.v7i2.3348

Tambunan, M., Panjaitan, B., & Siahaan, N. (2023). Legal Protection of Copyright Based on Law Number 28 Of 2014 Concerning Copyright. *Journal of Social Research*, *2*(4), 1355–1362.

https://doi.org/https://doi.org/10.55324/josr.v2i4.807

Tampubolon, I. R., Sudjana, U., & Cahyadini, A. (2020). Gerbang Pembayaran Nasional (GPN) Sebagai Instrumen Dalam Optimalisasi Penarikan Pajak Penghasilan (PPh) Pada Transaksi E-Commerce. *Jihk*, *1*(2), 90–106. https://doi.org/10.46924/jihk.v1i2.124

Thakur, T. (2024). Understanding Digital Copyright. *International Journal of Law Management & Humanities*, *7*(2), 2348–2356. https://doi.org/https://doij.org/10.10000/IJLMH.117240

Wibowo, A. (2023). *Internet of Things (IoT) dalam Ekonomi dan Bisnis Digital.* Penerbit Yayasan Prima Agus Teknik.

Yanti, I. (2023). Praktik Jual Beli Akun Spotify Premium Perspektif Kompilasi Hukum Ekonomi Syariah dan Hukum Positif. *Journal of Islamic Business Law*, *7*(2), 1–16. http://urj.uin-malang.ac.id/index.php/jibl/article/view/3249%0A

Yohanis et.al. (2020). *Manajemen Bisnis di Era Digital*. CV. Subaltern Inti Media.

Zaklylen, A. Z., Hanifah, M., & Lestari, R. (2025). Tinjauan Yuridis Wanprestasi Terhadap Perjanjian Jual Beli Akun Vidio Premium Milik Pt Vidio Oleh Pengguna Di Media Sosial Dan Marketplace. *Jurnal Ilmiah Wahana Pendidikan*, *11*(6.C), 17–32. https://jurnal.peneliti.net/index.php/JIWP/article/view/10696