

REGULATING ONLINE PLATFORMS IN MYANMAR- OBLIGATIONS, IMMUNITIES, AND LEGAL REFORM

Nang Myint Myat YADANAR¹

1 Faculty of Law, Chulalongkorn University, Bangkok, Thailand;
6784008234@student.chula.ac.th

ABSTRACT

This thesis examines the legal frameworks governing the regulation of online platforms in Myanmar, Indonesia, and the European Union, with particular emphasis on platform obligations, intermediary immunities, and liability for trademark infringement in digital marketplaces. The research aims to identify gaps in Myanmar's current regulatory framework, analyze comparative legal approaches adopted in Indonesia and the European Union, and propose targeted legal reforms for Myanmar. The study focuses on written laws, regulatory instruments, and judicial decisions relating to intermediary liability and online platform regulation. Employing a comparative legal methodology, the research analyzes primary legal sources through the two-pillar framework of Notice-and-Takedown obligations and Safe Harbor immunity, examining how each jurisdiction balances regulatory obligations imposed on online platforms with conditional immunity from liability. The comparative analysis demonstrates that Myanmar's current approach imposes takedown obligations on online platforms without providing corresponding safe harbor protections, thereby exposing compliant platforms to significant legal uncertainty and liability risks. Accordingly, the thesis argues for comprehensive legal reform to establish a more balanced and coherent framework for online platform regulation in Myanmar.

Keywords: E-commerce Platforms, Trademark Infringement, Intermediary Liability, Safe Harbor, Notice-and-Takedown, Myanmar, Indonesia, European Union, Digital Services Act

CITATION INFORMATION: Yadanar, N. (2026). Regulating Online Platforms in Myanmar-Obligations, Immunities, and Legal Reform. *Procedia of Multidisciplinary Research*, 4(7), 1.

INTRODUCTION

Global e-commerce has recently played an important role in driving the national economy and society's well-being, creating an interest for governments in promoting foreign investment to expand digital business opportunities. However, the most important thing for business entrepreneurs and policymakers is to be aware of unfamiliar business landscapes and environments, including economic, political, legal, and technological factors (OECD, 2020; Google et al., 2024). E-commerce platforms such as Amazon Marketplace, Shopee, Lazada, and Alibaba have become dominant forces in global trade, connecting millions of sellers with consumers across borders. These platforms facilitate fast transactions and broad connectivity, but their features also create conditions that enable intellectual property violations, particularly the sale of counterfeit trademark-infringing goods (OECD/EUIPO, 2021). The U.S. Department of Homeland Security (2020) revealed that the structure of global online marketplaces has been increasingly used by those seeking to distribute infringing or counterfeit goods. One of the biggest issues for international business and digital trade is the concern about platform liability for trademark infringement.

The United States pioneered the legal response to online intermediary liability with the Digital Millennium Copyright Act of 1998 (DMCA, 1998). Sablyar (2025) advocated that legal frameworks play a significant role in the business environment since they can help business entrepreneurs and platforms operate with legal certainty. The DMCA introduced a two-pillar framework: Notice-and-Takedown as the platform obligation, and Safe Harbor as the platform immunity. Under this system, platforms that remove infringing content upon receiving proper notice receive protection from monetary liability (17 U.S.C. § 512). This balance gives platforms the confidence to host user content while providing rights owners with an effective mechanism to protect their intellectual property. However, the DMCA applies only to copyright infringement. Goodyear (2025) revealed that the United States has not extended this statutory framework to trademark infringement, instead developing a common law standard under *Tiffany v. eBay* (2010) that requires specific knowledge of counterfeit listings before imposing liability.

The European Union has adopted a complete two-pillar framework for all forms of illegal content, including trademark infringement, through the Digital Services Act (DSA, 2022). Husovec (2023) advocated that the DSA represents the first comprehensive attempt to create a second generation of rules for digital services, separating accountability from liability. Indonesia has developed its own framework centered on Minister of Communication and Informatics Regulation No. 5 of 2020 (MOCI 5/2020), which provides ambiguous Safe Harbor protection and fixed takedown timeframes. Setiawan (2021) revealed that Indonesia's current framework leads to legal uncertainty for platforms since the permissive language "can be exempted" rather than "shall be exempted" leaves compliance without guaranteed protection. Myanmar presents a striking contrast. The country enacted a comprehensive Trademark Law in 2019 (Trademark Law, 2019), but this law focuses exclusively on direct infringers and contains no provisions on intermediary liability. Tilleke & Gibbins (2023) revealed that Myanmar's online enforcement mechanisms remain untested and rights holders face significant challenges in protecting their intellectual property online. To fill this gap, the Ministry of Commerce issued E-commerce Guidelines in September 2023 (E-commerce Guidelines, 2023). These Guidelines impose a Notice-and-Takedown obligation on platform entrepreneurs. However, they provide no corresponding Safe Harbor protection. A platform that diligently removes infringing content upon receiving a valid complaint remains exposed to potential liability. Myanmar thus presents a unique case of obligation without immunity.

This study investigates the legal frameworks governing e-commerce platform liability for trademark infringement in Myanmar, Indonesia, and the European Union. It addresses four research questions. First, what foundational legal concepts govern platform liability, including

direct and secondary liability and the two-pillar framework? Second, how do the three jurisdictions approach Safe Harbor protection? Third, how do their Notice-and-Takedown mechanisms compare in terms of procedural requirements and legal certainty? Fourth, what gaps exist in Myanmar's framework, and what reforms can comparative analysis suggest? The research adopts a doctrinal legal methodology combined with a comparative legal approach, examining primary sources including statutes, regulations, guidelines, and judicial decisions from all three jurisdictions up to 2026.

LITERATURE REVIEWS

The Nature of Platform Liability

In the e-commerce context, a platform functions as a digital intermediary that facilitates transactions between sellers and buyers. Unlike traditional retailers that purchase, own, and resell goods, platforms provide infrastructure such as websites, applications, and payment systems. The platform itself does not typically take title to the goods. Its role connects sellers to buyers. OECD (2020) revealed that the regulation of e-commerce platforms fundamentally depends on the legal concept of intermediary liability, the conditions under which an online service provider may be held accountable for trademark-infringing goods listed by its users. This unique position raises a fundamental question: when should a platform face legal responsibility for what an independent seller sells? Platform liability refers to the legal responsibility of an online intermediary for the actions of its users, specifically for trademark infringement committed by independent sellers offering counterfeit goods (Bird & Bird, 2022). Unlike the seller who directly infringes, the platform provides the marketplace but does not sell the counterfeit product itself. Platforms possess significant power to prevent or reduce infringement. Yet imposing excessive liability could lead platforms to remove lawful content to avoid legal risk. The challenge requires a middle ground: encouraging platforms to address infringement without overburdening them.

Types of Platform Liability

Platforms may face liability under two main categories: direct liability and secondary liability. Direct liability assigns legal responsibility to the intermediary as if it were the primary infringer (Baker Botts, 2025). This occurs when the platform itself sells counterfeit goods, takes ownership of products, or presents itself as the seller rather than a mere intermediary. The *Google France v. Louis Vuitton* (2010) case established that an intermediary does not face direct liability unless it plays an "active role" in the infringement. The Court of Justice of the European Union held that Google's role remained merely technical, automatic, and passive, thus exempting it from direct liability.

Secondary liability applies when the platform faces responsibility for infringement committed by others, such as independent sellers using its marketplace (Shukla, 2017). This category includes two main doctrines: contributory infringement and vicarious liability. Contributory infringement occurs when a party knowingly helps another person infringe (Northwest Registered Agent, 2023). The leading case, *Inwood Laboratories v. Ives Laboratories* (1982), established that a party may face liability if it intentionally induces another to infringe or continues supplying its product to someone it knows is engaging in infringement.

The *Tiffany v. eBay* (2010) case applied this doctrine to online marketplaces. The Second Circuit held that to face contributory liability, a platform must have specific knowledge of particular infringing listings, not merely general knowledge that counterfeiting occurs on its site. Goodyear (2025) revealed that this distinction is important: general knowledge does not trigger a duty to act, while specific knowledge does. However, the court also recognized an important exception: willful blindness. A platform cannot avoid liability by deliberately shielding itself from knowledge of infringement. The Second Circuit stated that willful blindness "is tantamount to actual knowledge" under trademark law (Goodyear, 2025, p. 110).

Vicarious liability focuses on control and financial benefit rather than knowledge. The Legal Information Institute (n.d.) defined vicarious liability as a form of secondary liability that holds one person responsible for the infringing acts of another based on their relationship. A party may be held vicariously liable for trademark infringement if it has the right and ability to control the infringing activity and receives a direct financial benefit from that activity (Bartholomew & Tehranian, 2006). The *Fonovisa v. Cherry Auction* (1996) case held a swap meet operator vicariously liable for vendors selling counterfeit goods because the operator exercised control and profited from admissions and parking fees. This reasoning applies directly to e-commerce platforms.

The Two-Pillar Framework

Notice-and-Takedown constitutes the obligation pillar. Sablyar (2025) revealed that under the Digital Millennium Copyright Act (DMCA, 1998), when a copyright owner submits a valid notice identifying infringing material, the platform must remove or disable access. Safe Harbor constitutes the immunity pillar. It protects platforms from civil liability for their users' infringing acts when platforms comply with their obligations. The two-pillar framework connects directly: the obligation serves as the condition, and immunity serves as the reward. Husovec (2023) advocated that the Digital Services Act (DSA, 2022) separates accountability from liability, creating self-standing regulatory expectations that are enforced separately.

However, the DMCA's two-pillar framework applies only to copyright infringement. Goodyear (2025) revealed that the United States has not created a similar law for trademark infringement. Instead, US courts have developed a common law Notice-and-Takedown system for trademark under *Tiffany v. eBay* (2010). One scholar describes this as the "third, more opaque and less scrutinized regime" (Goodyear, 2025, p. 107). This means the US does not use the statutory two-pillar framework for trademark. The EU does through the Digital Services Act (DSA, 2022). This difference helps explain how the US model has been adapted differently across jurisdictions.

RESEARCH METHODOLOGY

This research adopts a doctrinal legal methodology combined with a comparative legal approach. Doctrinal legal research involves the systematic analysis of primary legal sources including statutes, regulations, guidelines, and judicial decisions. The comparative method allows for the functional examination of how different jurisdictions address the common problem of platform liability for trademark infringement.

The three jurisdictions were selected to represent different points on the spectrum of legal transplantation. The European Union represents a complete model, having adopted the Digital Services Act (2022) which provides clear statutory obligations paired with conditional immunity covering both copyright and trademark infringement. Indonesia represents a developing framework, having established Notice-and-Takedown procedures with ambiguous Safe Harbor protection and fixed takedown timeframes under MOCI 5/2020 and Regulation 47/2025. Myanmar represents an incomplete case of "obligation without immunity," where the E-commerce Guidelines (2023) impose takedown duties but provide no corresponding Safe Harbor protection. This spectrum allows for meaningful comparison of how the same US DMCA model has been adapted differently across jurisdictions.

The comparative analysis examines three variables across all three jurisdictions: (1) Safe Harbor protection, including legal basis, nature of protection, and certainty of immunity; (2) Notice-and-Takedown procedures, including notice requirements and takedown timeframes; and (3) additional features such as trusted flagger systems, transparency databases, and government-led pathways. These variables are derived from the two-pillar framework of the US DMCA, which serves as the analytical lens throughout the study.

The study examines primary legal sources including the EU Digital Services Act (Regulation (EU) 2022/2065), Indonesia's MOCI 5/2020 and Regulation 47/2025, Myanmar's Trademark Law (2019) and E-commerce Guidelines (2023), as well as relevant court decisions including *Google France v. Louis Vuitton* (2010), *Tiffany v. eBay* (2010), and *Skinport v. Google* (2025). Secondary sources include scholarly articles, law firm publications, and policy briefs.

This study addresses civil liability only; criminal dimensions of trademark infringement are acknowledged but not analyzed in depth. The focus is limited to e-commerce platforms that host third-party sellers. The recent nature of Myanmar's E-commerce Guidelines (2023) and Indonesia's Regulation 47/2025 means that judicial interpretation and enforcement practice are not yet available. This study is therefore doctrinal rather than empirical.

RESEARCH RESULTS

The European Union: Complete Framework

The European Union provides the most complete platform liability framework under the Digital Services Act (DSA, 2022). Article 6 establishes conditional Safe Harbor immunity. A hosting provider faces no liability for illegal content stored at a user's request if it lacks actual knowledge of the illegal activity or, upon obtaining such knowledge, acts expeditiously to remove or disable access to the content. Husovec (2023) advocated that the DSA represents the first comprehensive attempt to create a second generation of rules for digital services. Article 7 encourages voluntary proactive measures by ensuring that platforms do not lose Safe Harbor eligibility simply because they conduct voluntary investigations. Article 8 confirms that platforms face no general obligation to actively monitor all hosted content.

For Notice-and-Takedown, Article 16 requires every hosting service provider to establish a user-friendly notice system. A valid notice must contain four elements: a clear explanation of why the content is illegal, the exact electronic location (URL), the reporter's name and email address, and a good faith statement confirming accuracy and completeness (DSA, 2022). A valid notice gives the platform actual knowledge of illegal content, triggering the obligation to act expeditiously. Article 17 requires platforms to provide clear statements of reasons to affected users.

The first major court decision on platform liability under the DSA involved a trademark dispute between *Skinport v. Google* (Maucher Jenkins, 2025). The Düsseldorf Regional Court held that Google was liable as a "disruptive party" (Störerhaftung). Once Google received a sufficiently specific notice from Skinport, it obtained actual knowledge of the trademark violation (Heise online, 2025). This knowledge triggered an obligation not only to remove the specific infringing ad but also to take reasonable measures to prevent similar future infringements.

Beyond the standard Notice-and-Takedown mechanism, the DSA creates trusted flaggers, entities with special expertise in detecting illegal content whose notices receive priority processing (DSA, 2022, Article 22). CMS Law (2025) revealed that trusted flaggers must demonstrate special expertise, maintain independence from any online platform, and carry out activities diligently and objectively. Article 24(5) establishes a publicly accessible transparency database where platforms submit all statements of reasons, enabling external monitoring of content moderation decisions (DSA, 2022). Groesch et al. (2026) revealed that this database allows researchers to check whether platforms follow the rules.

Indonesia: Layered and Ambiguous Framework

Indonesia's framework rests on Minister of Communication and Informatics Regulation No. 5 of 2020 (MOCI 5/2020). Article 11 establishes Safe Harbor, providing that platforms "can be exempted" from legal responsibility for user content if they fulfill three conditions: compliance with governance obligations, provision of subscriber information to authorities, and takedown of prohibited content upon receiving complaints (MOCI 5/2020). However, the permissive

language "can be" rather than "shall be" introduces significant ambiguity. Setiawan (2021) revealed that compliance does not guarantee immunity, leaving platforms in legal uncertainty. Under Article 10(4)(b) of MOCI 5/2020, platforms must conduct an "independent examination" of each complaint. This requirement forces platforms to make legal judgments about whether content constitutes trademark infringement. The Korean Internet Governance Observatory (2020) revealed that a platform that makes an incorrect judgment could face liability for that wrong decision. This liability-imposing framework undermines the protective purpose of Safe Harbor.

For Notice-and-Takedown, the Circular Letter accompanying MOCI 5/2020 specifies timeframes. For intellectual property infringement, platforms must act within 14 calendar days (Circular Letter 5/2016). A valid complaint must include the reporter's identity, reasons why the content is prohibited, and supporting evidence such as trademark registration certificates. Rouse (2025) revealed that in practice, platforms may not stick to the 14-day timeframe. The Circular Letter also provides a counter-notice mechanism allowing sellers to object within 7 days (Circular Letter 5/2016).

Indonesia also created a government-led pathway under Regulation 47/2025, allowing rights holders to submit reports directly to the Directorate General of Intellectual Property (Regulation 47/2025). A verification team examines the report within 3 days. If infringement is proven, the team can recommend partial site closure, full site closure, or access termination (Makarim & Taira S., 2026). Rajah & Tann Asia (2026) revealed that this dual pathway operates much faster than the 14-day platform deadline.

Myanmar: Missing Pillar

Myanmar sits at the extreme end of the spectrum. The Trademark Law (2019) contains no provisions on intermediary liability. It provides remedies against direct infringers but says nothing about online platforms. The E-commerce Guidelines (2023) impose a takedown obligation on platform entrepreneurs but provide no Safe Harbor protection. Tilleke & Gibbins (2023) revealed that failure to comply results in the platform having "the same responsibility for the infringement as the relevant e-commerce entrepreneur," effectively treating the platform as a direct infringer.

The Guidelines define three situations that constitute knowledge or failure to act (E-commerce Guidelines, 2023). First, if a platform knows about infringement but does nothing to stop it. Second, if a platform does not have proper measures in place to protect intellectual property rights. Third, if a platform promotes or distributes information about infringing products to boost sales. The Guidelines include a 7-day response period for sellers to object and a 30-day period for legal action. However, they do not specify a timeframe for platform takedown. They do not define what constitutes a valid notice. They provide no independent appeal mechanism for sellers.

Unlike the EU's binding regulation or Indonesia's ministerial regulation, the Guidelines are soft law, issued as administrative guidance rather than binding legislation. Asia IP (2023) revealed that the Guidelines themselves acknowledge they are "not yet enforced as law." Boswald (2025) advocated that soft law must complement, not replace, binding regulation because voluntary measures alone cannot change platform behavior. This soft law status creates uncertainty. This incomplete framework creates obligation without immunity, leaving compliant platforms exposed to liability.

Spectrum of Safe Harbor Protection

The comparative analysis reveals a clear spectrum of Safe Harbor protection across the three jurisdictions. The European Union stands at one end with complete protection. Husovec (2023) revealed that the DSA provides conditional and automatic immunity upon compliance. Indonesia occupies a middle position. Setiawan (2021) revealed that Indonesia's Safe Harbor framework is implicit rather than explicit, with the permissive language "can be exempted"

rather than "shall be exempted" creating legal uncertainty. Myanmar sits at the opposite end with no Safe Harbor protection whatsoever. Tilleke & Gibbins (2023) revealed that Myanmar offers no legal shield to exempt a platform from liability for user content.

Obligation Without Immunity

The central finding of this study is that Myanmar presents a unique case of obligation without immunity. The US DMCA model pairs two pillars together: Safe Harbor immunity as the reward and Notice-and-Takedown obligation as the condition. Myanmar has adopted the second pillar but not the first. The E-commerce Guidelines (2023) impose a takedown obligation but provide no Safe Harbor protection. A platform that diligently removes infringing content remains exposed to potential liability. Unlike the EU's binding regulation or Indonesia's ministerial regulation, Myanmar's Guidelines are soft law (Asia IP, 2023).

Comparison of Notice-and-Takedown Procedures

The three jurisdictions differ significantly. The EU requires four specific elements for a valid notice: explanation of illegality, exact URL, reporter's identity, and good faith statement (DSA, 2022). Indonesia requires the reporter's identity, reasons for prohibition, and supporting evidence (Circular Letter 5/2016). For intellectual property infringement, platforms must act within 14 calendar days (Rouse, 2025). Myanmar provides no clear notice requirements and no timeframe for takedown. The E-commerce Guidelines (2023) contain a 7-day response period for the seller to object, but no deadline for the platform to remove content.

Consequences of Incomplete Transplantation

The incomplete framework in Myanmar creates several negative consequences. First, platforms have no incentive to invest in content moderation systems (Tilleke & Gibbins, 2023). Second, rights holders lack effective tools to enforce their trademark rights. Third, foreign investment faces discouragement due to legal uncertainty. EuroCham Myanmar (2022) revealed that international businesses seek legal certainty before entering new markets. Fourth, the digital economy suffers. The World Intellectual Property Organization (2021) revealed that e-commerce cannot grow without clear rules. Myanmar risks being left behind as Southeast Asia's digital economy continues to grow rapidly.

CONCLUSION AND DISCUSSION

Summary of Findings

This study investigated the legal frameworks governing e-commerce platform liability for trademark infringement in Myanmar, Indonesia, and the European Union. The comparative analysis reveals three distinct models. The European Union offers the most complete framework, with conditional and automatic Safe Harbor protection upon compliance, detailed notice requirements, and additional features such as trusted flaggers and a transparency database (DSA, 2022; Husovec, 2023). Indonesia occupies a middle position, with fixed 14-day timeframes for trademark infringement takedown and a government-led pathway under Regulation 47/2025, but its ambiguous Safe Harbor language creates legal uncertainty (Setiawan, 2021; MOCI 5/2020). Myanmar sits at the opposite end with no Safe Harbor protection, no secondary liability, and only soft law guidelines. The E-commerce Guidelines (2023) impose takedown obligations but grant no immunity, creating a situation of obligation without immunity (Tilleke & Gibbins, 2023).

Recommendations for Myanmar

Based on the comparative findings, this study offers four specific recommendations for Myanmar. These recommendations are grounded in the central puzzle identified in the thesis, Myanmar's "obligation without immunity" framework, and acknowledge the current political and administrative realities that make legislative action challenging.

First, Myanmar needs a complete two-pillar framework that combines Safe Harbor protection with clear Notice-and-Takedown procedures. The framework should include the following

elements. A Safe Harbor provision stating that platforms which comply with Notice-and-Takedown obligations shall not be held civilly liable for third-party trademark infringement. Safe Harbor provisions are essential for creating legal certainty and encouraging platforms to cooperate with rights holders (Frosio & Geiger, 2024). Clear notice requirements specifying what information a rights holder must provide when reporting infringement. This includes a description of the alleged infringement and the location of the content, as well as the identity of the person submitting the notice and a confirmation of good faith. These general requirements follow the EU model under Article 16 of the DSA. Clear notice requirements ensure that platforms receive precise and reliable information about alleged infringement (Groesch et al., 2026). A requirement that notices include supporting evidence, such as trademark registration certificates. This follows the general approach of Indonesia's Circular Letter. Clear notice requirements would help platforms verify complaints quickly and help rights holders submit effective complaints. By establishing clearer rules, a stable legal environment can foster innovation and growth (Frosio & Geiger, 2024). Myanmar needs the same clarity. The exact details can be adapted to Myanmar's legal context. The key principle is simple: rights holders should know what information to provide and platforms should know what to expect in a valid notice.

Second, Myanmar should adopt fixed timeframes through administrative order. Following Indonesia's model under MOCI 5/2020, Myanmar should establish a clear 14-day deadline for platform takedown of trademark-infringing content through a ministerial notification. Unlike the EU's flexible "without undue delay" standard, a fixed 14-day timeframe would give rights holders a predictable timeline and platforms a specific target to meet, reducing the current legal uncertainty.

Third, Myanmar should establish a centralized enforcement authority within existing administrative structures. To remedy the current absence of any enforcement mechanism, Myanmar should designate the Intellectual Property Department or the Department of Trade as the single point of contact for receiving complaints, investigating violations, and coordinating with platforms. This recommendation draws from Indonesia's Regulation 47/2025, which created a government-led takedown pathway, providing an alternative to platform-based Notice-and-Takedown.

Fourth, Myanmar should develop a phased approach to trusted flagger and transparency mechanisms. In the short term, Myanmar should focus on building basic administrative capacity and enforcing fixed timeframes. In the medium term, as political conditions stabilize, Myanmar should pursue comprehensive legislative reform to enact a complete two-pillar framework, ideally adopting additional features from the EU Digital Services Act, including a trusted flagger system for priority processing of expert notices and a public transparency database for accountability. These advanced features represent best practices that Myanmar can work toward as its e-commerce ecosystem and administrative capacity mature.

Concluding Remarks

The two-pillar framework matters because it balances the interests of platforms, rights holders, and users. Platforms need legal certainty to invest in content moderation. Rights holders need effective tools to enforce their trademarks. Users need protection against wrongful takedowns and counterfeit goods. Without both pillars, Safe Harbor immunity paired with Notice-and-Takedown obligation, the system becomes unbalanced and unfair. Myanmar's current framework of obligation without immunity exemplifies this imbalance, leaving compliant platforms exposed to liability and rights holders without effective remedies.

Myanmar has an opportunity to learn from the European Union and Indonesia. The EU provides a model of a complete framework under the Digital Services Act, with conditional Safe Harbor (Article 6), voluntary proactive measures (Article 7), and robust transparency mechanisms. Indonesia provides examples of fixed timeframes (14 days for IP infringement)

and a government-led pathway under Regulation 47/2025, offering an alternative to platform-based enforcement. However, Myanmar must adapt these models to its current political and administrative realities. The E-commerce Guidelines are soft law, not a binding statute.

Myanmar should focus on achievable administrative reforms that build toward a complete legal framework over time. The Ministry of Commerce should amend the existing Guidelines to add a Safe Harbor provision, adopt fixed 14-day takedown timeframes, designate a centralized enforcement authority, and pursue a phased approach toward trusted flagger and transparency mechanisms. Only then will platforms have legal certainty. Only then will rights holders have effective protection. Only then will Myanmar's digital economy reach its full potential.

REFERENCES

- Asia IP. (2023). *Myanmar establishes guidelines for the new registration requirements for ecommerce*.
- Baker Botts. (2025). *On-line platform liability for third-party trademark infringement* [Legal update].
- Bartholomew, M., & Tehranian, J. (2006). *The secret life of legal doctrine: The divergent evolution of secondary liability in trademark and copyright law*. Berkeley Technology Law Journal, 21.
- Bird & Bird. (2022). *These shoes are made for walking: CJEU clarifies platform operators' trademark infringement liability*. BrandWrites.
- Boswald, L. M. (2025). *Soft law, hard risks? Co-regulation and risk mitigation under the Digital Services Act* (Policy brief). interface.
- Circular Letter No. 5 of 2016 on Limitations and Responsibilities of Platform Providers and Merchants in Electronic Commerce Using User-Generated Content Platforms. (2016). Ministry of Communication and Informatics, Indonesia.
- CMS Law. (2025). *The first trusted flagger appointed under the DSA in Italy*.
- Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (1998).
- Digital Services Act, Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services (2022).
- E-commerce Guidelines, Export/Import Bulletin No. 1/2023, Ministry of Commerce, Myanmar (2023).
- EuroCham Myanmar. (2022). *The transformation of Myanmar's intellectual property (IP) system - What's in store for small and medium-sized enterprises (SMEs)?*
- Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259 (9th Cir. 1996).
- Frosio, G., & Geiger, C. (2024, February 20). *Towards a digital constitution: How the Digital Services Act shapes the future of online governance*. VerfBlog.
- Google France SARL v. Louis Vuitton Malletier SA, Joined Cases C-236/08, C-237/08, C-238/08 (Court of Justice of the European Union, 2010).
- Goodyear, M. P. (2025). *Common law notice-and-takedown*. NYU Journal of Intellectual Property & Entertainment Law, 15(1), 105-145.
- Google, Temasek, & Bain & Company. (2024). *e-Conomy SEA 2024: Profits on the rise, harnessing SEA's advantage*.
- Griffin, R. (2025). *Procedural fetishism in the Digital Services Act*. European Journal of Legal Studies, Special Issue, 15-40.
- Groesch, S., Birrer, A., Just, N., & Saurwein, F. (2026). *Big data, small answers: How the DSA transparency database falls short of its regulatory objectives*. Telecommunications Policy, 50(2), 1-15.
- Heise online. (2025). *Ruling: Google liable for fraudulent ads as a disruptive party under the DSA*.
- Husovec, M. (2023). *Rising above liability: The Digital Services Act as a blueprint for the second generation of global internet rules*. Berkeley Technology Law Journal, 38(2), 100-150.
- Inwood Laboratories, Inc. v. Ives Laboratories, Inc., 456 U.S. 844 (1982).
- Korean Internet Governance Observatory. (2020). *Dangers of notice-and-takedown as liability not a safe harbor in Indonesia*. Open Net Korea.
- Legal Information Institute. (n.d.). Vicarious infringement. *Wex Legal Dictionary*.
- Makarim & Taira S. (2026). *Building digital defenses: Indonesia's new framework for IPR protection in electronic systems*.
- Maucher Jenkins. (2025). *Digital service act & trademarks on platforms*.

- Minister of Communication and Informatics Regulation No. 5 of 2020 on Electronic System Operator in Private Sectors, Indonesia (2020).
- Minister of Law Regulation No. 47 of 2025 on the Handling of Intellectual Property Infringement Reports in Electronic Systems, Indonesia (2025).
- Northwest Registered Agent. (2023). Trademark infringement.
- OECD. (2020). *Guide for addressing the challenges of the digital economy: Intermediary liability*. OECD Publishing.
- OECD/EUIPO. (2021). *Global trade in fakes: A worrying threat. Illicit trade*. OECD Publishing.
- Pyidaungsu Hluttaw Law No. 3, 2019. The Trademark Law, Myanmar (2019).
- Rajah & Tann Asia. (2026). *New framework for addressing IP infringement on digital platforms under Minister of Law Regulation No. 47 of 2025*.
- Rouse. (2024). *Social media in Indonesia: What brand owners need to know*.
- Rouse. (2025). *Indonesia: E-commerce platform liability and safe harbor provisions*.
- Sablyar, T. (2025). *Adapting copyright law for the digital age: A review of the role and impact of the Digital Millennium Copyright Act*.
- Setiawan, I. (2021). *Who is responsible for user-generated content on digital platforms in Indonesia?* (Policy Brief). Center for Indonesian Policy Studies.
- Shukla, S. (2017). *Liability of online market portals vis-à-vis trademark infringement in the cyberspace*. IIPRD.
- Skinport v. Google* (Düsseldorf Regional Court, 2025).
- Tiffany (NJ) Inc. v. eBay Inc.*, 600 F.3d 93 (2d Cir. 2010).
- Tilleke & Gibbins. (2023). *Myanmar issues guidelines for e-commerce businesses*.
- U.S. Department of Homeland Security. (2020). *Combating trafficking in counterfeit and pirated goods: Report to the President of the United States*.
- World Intellectual Property Organization. (2021). *The impact of e-commerce on IP enforcement*.
- 17 U.S.C. § 512 (2018). Limitations on liability relating to material online.

Data Availability Statement: The raw data supporting the conclusions of this article will be made available by the authors, without undue reservation.

Conflicts of Interest: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.



Copyright: © 2026 by the authors. This is a fully open-access article distributed under the terms of the Attribution-NonCommercial-NoDerivatives 4.0 International (CC BY-NC-ND 4.0).