

General Monitoring Obligations in Thailand:
A Reform Proposal Based on the Mere
Conduit Principle and Insights from
China and beyond

Peeyakorn Leankattava

General Monitoring Obligations in Thailand: A Reform Proposal Based on the Mere Conduit Principle and Insights from China and beyond*

Peeyakorn Leankattava **

Abstract

Globally, intermediary-liability frameworks seek to balance freedom of expression, national security, and privacy by limiting monitoring obligations. However, Thailand's Computer-Related Crime Act imposes proactive obligations, raising concerns over disproportionate burdens. This study proposes adopting the mere conduit principle from private law to balance freedom of expression with national security and privacy obligations in Thailand. We recommend: (1) clearly defining the mere conduit principle; (2) implementing a case-specific approach to takedown requests that consider intermediaries' size and technological capacity; and (3) requiring court orders for national security-related takedowns while permitting individual notice mechanisms for privacy-related obligations.

Keywords: china intermediary liability, mere conduit principle, thailand media regulation

***Acknowledgments:** I wish to express my profound gratitude to Professor Dr. Shen Wei, Professor Dr. Daniel Allan Rosen, Associate Professor Dr. Rawin Leelapatana, Associate Professor Dr. Thanapat Chatinakrob, Ms. Thitirat Thipsamritkul, Professor Tyrell Haberkorn, Associate Professor Dr. Jompon Pitaksantayothin, Associate Professor Sawatree Suksri, Professor Thongchai Winichakul, and Dr. Kitjapat Kesiranon for their meticulous review and insightful commentary on my draft. I am also indebted to Wu, Zhang, Pigeon, Eddie, Ex, Alex, Marie, Peter, YY, Prasit, and James for their invaluable inspiration, motivation, and unwavering support.

****** Lecturer in Law at Faculty of Law, Ramkhamhaeng University; Doctor of Juridical Science candidate, KoGuan Law School, Shanghai Jiao Tong University, China. E-mail: pang_piyakorn@hotmail.co.th

Received 28 September 2025, Revised 18 February 2026, Accepted 19 February 2026.

1. Introduction

Internet intermediaries such as Facebook operate as infrastructural states, supporting democratic culture and free speech while simultaneously navigating regulatory frameworks that intersect with political, legal, and technological challenges.¹ Regulating online speech has become a complex interplay among private entities, regulatory authorities, and judicial bodies, in which intermediary-liability frameworks define platform responsibility for third-party content.

Globally, intermediary-liability frameworks grant immunity to intermediaries that neither modify nor have actual knowledge of illegal content, while prohibiting general monitoring obligations.² According to Timmermans, individuals who act as a “mere conduit” enjoy almost full immunity.³ This has been widely recognized as the mere conduit paradigm in international regulatory regimes, such as those enshrined in Articles 12-14 of the European Union (EU) E-Commerce Directive (2000/31/EC) an approach influenced by the United States’ legal principles-underpinning content-moderation laws addressing hate speech, national security threats, and privacy violations.⁴ This principle frames the recognition and support of freedom of expression (FOE), legal certainty, and the functional neutrality of the digital infrastructure.

¹Kate Klonick, “The New Governors: The People, Rules, and Processes Governing Online Speech,” *Harvard Law Review* 131, 6 (2018): 1603.

²Aleksandra Kuczerawy, “From ‘Notice and Take Down’ to ‘Notice and Stay Down’”: Risks and Safeguards for Freedom of Expression,” in *The Oxford Handbook of Intermediary Liability Online*, edited by G. Frosio (Oxford: Oxford University Press, 2019), pp. 524–543.

³Louise Timmermans, “The Role of Internet Intermediaries in the Protection of Freedom of Expression and Personal Data: Human Rights in a Digital Age,” (Master’s thesis, University of Montpellier, 2017), p. 18.

⁴Baiyang Xiao, “Making the Private Public: Regulating Content Moderation under Chinese Law,” *Computer Law and Security Review* 51 (2023): 1–16.; Moreover, Pimton defines a mere-conduit as per the EU E-Commerce Directive (2000/31/EC). See C. Pimton, *Liability of Service Providers as Intermediaries: Notification of Computer Data Suspension and Removal from Computer Systems* (Bangkok: Chulalongkorn University, 2018), pp. 38–39.

However, Thailand's regulatory approach lacks a coherent framework, causing it to differ substantially from this global trend. This divergence has not been comprehensively examined by Thai scholars. Therefore, this study uses a doctrinal and comparative analysis of primary case studies from Thailand and insights from China's dual-track approach to bridge this gap. In doing so, it addresses a critical question: What constitutes a proportionate and legitimate legal framework for intermediaries' monitoring obligations in Thailand that balances FOE with (1) national security and (2) privacy protection while fostering technological advancements?

The enforcement of Thailand's Computer-Related Crime Act (CCA) and *lèse-majesté* laws illustrates the increasingly complex relationships among intermediaries, the state, and citizens. During the 2017 and 2020 pro-democracy movements in Thailand, the Thai government threatened Facebook with criminal liability and potential platform shutdowns unless it removed content deemed sensitive, particularly under *lèse-majesté* laws.⁵ Although such incidents have become less frequent, *lèse-majesté* laws continue to suppress political discourse and FOE.⁶ Data from Thai Lawyers for Human Rights reveal that as of 2024, over 1,947 individuals have been politically persecuted

⁵International Commission of Jurists, **Dictating the Internet: Curtailing free expression and information online in Thailand** [Online], available URL: <https://www.icj.org/wp-content/uploads/2021/06/Thailand-Dictating-the-Internet-FoE-Publication-2021-ENG.pdf>, 2021 (April); Komsan Tortermvasana and Online Reporters, **Facebook Faces Immediate Shutdown Threat** [Online], available URL: <https://www.bangkokpost.com/thailand/politics/1250114/facebook-faces-immediate-shutdown-threat>, 2017 (May, 16).

⁶Pattamon Anansaringkarn and Ric Neo. "How Can State Regulations over the Online Sphere Continue to Respect the Freedom of Expression? A Case Study of Contemporary 'Fake News' Regulations in Thailand," **Information and Communications Technology Law** 30, 3 (2021): 292; Southeast Asian Press Alliance. **SEAPA Submission to Study on Social Media, Search, and Freedom of Expression** [Online], available URL: <https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/ContentRegulation/Seapa.pdf>, n.d; Peter Leyland, "The Struggle for Freedom of Expression in Thailand: Media Moguls, the King, Citizen Politics and the Law," **Journal of Media Law** 2, 1 (2010): 115.

across 1,268 cases for sharing texts and photos on social media.⁷ The *Prachatai* case (Red No. 2091/2555) represents a watershed moment in Thai jurisprudence, as it is the first judicial interpretation of Article 15 of the CCA. The court found *Prachatai*'s editor liable for failing to remove user-generated content deemed offensive under *lèse-majesté* laws.⁸ Recognized by the United Nations and Judge Rapeeporn Wattanachiwakul,⁹ this case underscores the disproportionate burdens imposed by strict liability frameworks.¹⁰

Furthermore, the trend of platform liability is evident in Thailand and Malaysia. In 2023, the Malaysian Communications and Multimedia Commission announced legal action against Meta for failing to comply with content-takedown requests.¹¹ This reflects the broader global tensions among state control, platform governance, and individual

⁷TLHR, **Statistics of Lèse Majesté Cases with Court Rulings in Thailand** [Online], available URL: <https://tlhr2014.com/archives/46268>, 2022 (March, 28); TLHR, **January 2024: A Total of 1,947 People Has Been Politically Prosecuted Resulting in 1,268 Lawsuits** [Online], available URL: <https://tlhr2014.com/en/archives/64902>, 2024 (February, 19).

⁸ILaw, **Chiranuch Premchaiporn: Director of Prachatai** [Online], available URL: <https://www.ilaw.or.th/articles/case/23450>, 2016 (December, 2); Prachatai, **“Netizen Network: Summary of Movements Internet Case and the Liability of the Intermediary ‘Director of Prachatai’** [Online], available URL: https://prachatai.com/journal/2012/04/40258?__cf_chl_rt_tk=ROeVBqo5Fo9moenYiJAeBh09Bs2_hF0Sn08NHP5_SUQ-1700208807-0-gaNycGzNEtA, 2012 (April, 27).

⁹Rapeeporn Wattanachiwakul, “Liability Issues of Internet Service Providers as ‘Intermediaries’ under the Computer-Related Crime Act B.E., 2550.” Judicial Official Development Institute, Office of the Judiciary, 2014: 3, 26-27.

¹⁰Frank La Rue, **Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression** [Online], available URL: <https://digitallibrary.un.org/record/706200?v=pdf>, 2011 (May, 27).

¹¹Fuad Nizam, **MCMC to Take Legal Action Against Meta over Noncooperation to Remove Undesirable Contents from its Platform** [Online], available URL: <https://www.nst.com.my/news/crime-courts/2023/06/923358/mcmc-take-legal-action-against-meta-over-non-cooperation-remove>, 2023 (June, 23); Baiyang Xiao, op. cit., p. 1.

rights, especially as intermediaries should not be transformed into *de facto* censors.¹² Meanwhile, Thailand presents a particularly relevant case study, as it is an emerging jurisdiction in Southeast Asia that vividly illustrates the tensions between digital rights and state control, yet it lacks the jurisprudential safeguards typically found in liberal democratic societies. This study advances existing scholarship by examining how the mere conduit principle (MCP) has been understood and developed in Thailand and examines whether its interpretation aligns with international norms, deviates from them, or reflects unique regulatory characteristics shaped by its political and legal context.

A core challenge in Thailand's intermediary-liability framework is determining whether legal obligations unduly burden platforms, deterring free expression or incentivizing excessive compliance. This study applies Scanlon's legitimacy framework,¹³ which evaluates whether restrictions on FOE can be justified as legitimate and necessary, alongside Schauer's chilling effect theory,¹⁴ which addresses whether regulations create incentives for excessive censorship by intermediaries. These are considered in conjunction with Balkin's theory of technological infrastructure and FOE.¹⁵ Based on this framework, this study addresses how platform governance is shaped by state-imposed legal obligations. It shows that Thailand's intermediary-liability laws, as applied in the *Prachatai* case and Facebook takedown disputes, fail to meet the proportionality threshold, often lacking procedural safeguards in both national security and privacy contexts. Moreover, it sheds light on how unclear legal guidelines incentivize self-censorship, compelling platforms to over-remove content out of fear of liability, thereby undermining FOE and due process protections.

¹²*Ibid.*, p. 3.

¹³Thomas Scanlon, "A Theory of Freedom of Expression," *Philosophy and Public Affairs* 1, 2 (1972): 204–226.

¹⁴Frederick Schauer, "Fear, Risk and the First Amendment: Unraveling the Chilling Effect," *Boston University Law Review* 58 (1978): 685–732.

¹⁵Jack M. Balkin, "Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society," *New York University Law Review* 79, 1 (2004).

Regarding Chinese cases, although China's notice-and-takedown system primarily safeguards privacy rights, it also integrates a functionalist comparative-law perspective, giving it broader implications for Thailand's national security framework. This study examines whether the globally recognized MCP can be adapted to Thailand's regulatory environment. Xiao¹⁶ observed that the MCP, even in its EU formulation, provides a horizontal approach applicable across various categories of illegal content. This supports the comparative legal hypothesis that "the most private could at the same time be the most public."¹⁷

Despite growing scholarly interest in intermediary liability in Thailand, no studies have systematically compared Thailand's notice-and-takedown measures with those of China, specifically vis-à-vis national security and privacy. While some studies have focused on fake news regulation and others have criticized the notice-and-takedown measures of Internet intermediaries in Thailand,¹⁸ they have primarily addressed the notification of the Ministry of Digital Economy and Society Re: Procedures for Notification, Suspension of Dissemination of Computer Data, and Removal of Computer Data from Computer Systems 2017 (hereafter, Notification 2017).¹⁹ The present study examines the more recent Notification of the Ministry of Digital Economy and Society Re: Procedures for Notification, Suspension of Dissemination of Computer Data, and Removal of Computer Data from Computer Systems 2022 (hereafter, Notification 2022).²⁰

¹⁶Baiyang Xiao, op. cit., p. 2.

¹⁷Mark Van Hoecke, *Epistemology and Methodology of Comparative Law* (UK: Bloomsbury Publishing, 2004), p. 86.

¹⁸Pattamon Anansaringkarn and Ric Neo, op. cit.; Pimton, Liability of Service Providers as Intermediaries, abstract, 3.

¹⁹Royal Thai Government. Notification of the Ministry of Digital Economy and Society Re: Procedures for notification, suspension of dissemination of computer data, and removal of computer data from computer systems, 22 July 2017.

²⁰Royal Thai Government. Notification of the Ministry of Digital Economy and Society Re: Procedures for notification, suspension of dissemination of computer data, and removal of computer data from computer systems, 26 October 2022.

Wattanachiwakul²¹ explores the CCA's relationship with the European Union, United Kingdom, and United States frameworks; however, no study has systematically analyzed the intersection between the Thai and Chinese regulatory frameworks. Meanwhile, Chinese studies have focused on copyright issues,²² leaving a gap in intermediary-liability research concerning national security and privacy.

Thus, this study advances the discussion on whether the MCP is an efficient global standard for balancing FOE with national security and privacy rights across jurisdictions. It analyzes the historical development of Thailand's intermediary-liability framework, emphasizing the Memorandum of the Office of the Council of State as a crucial, yet underexplored, primary source of legislative intent behind the CCA.

This study contributes to the *de lege ferenda* discourse by advocating for the MCP's adoption within Thailand's legal framework to enhance legal predictability and proportionality in intermediary liability. While the MCP is rooted in private law, it has gained recognition in Chinese public law, suggesting broader regulatory potential.²³

This study identifies several critical gaps in Thailand's regulatory framework. First, the application of the MCP is inconsistent, despite its formal recognition under Notification 2022. Second, regulations regarding privacy-related issues are inadequate. Third, rigid takedown deadlines under the CCA disproportionately burden smaller platforms. Finally, judicial oversight is absent in national security cases.

To address these challenges, this article proposes several reforms. First, Thailand must explicitly define a "mere conduit." Second, notice-and-takedown procedures should be flexible and context-sensitive, accounting for platforms' size and technological capacity. Finally, judicial oversight should be mandated for national security-related takedowns.²⁴

²¹Rapeeporn Wattanachiwakul, op. cit., p. 4.

²²Tianxing He. "Online Content Platforms, Copyright Decision-making Algorithms and Fundamental Rights Protection in China," **Law Innovation and Technology** 14, 1 (March 2022): 71–94; Baiyang Xiao, op. cit.

²³Ibid., p. 1.

²⁴Aleksandra Kuczerawy, op. cit.

2. A Theoretical Framework of Intermediary Liability in Thailand: Lessons from China and Beyond

2.1 Regulatory Framework and Thailand's Current Regulatory Environment

2.1.1 National Security Aspects of Proactive Monitoring and Government Censorship

Thailand's regulatory framework for Internet intermediaries is grounded in strict liability under the CCA. Section 5 of Notification 2022 articulates the MCP, exempting intermediaries from liability if they fully comply with Sections 5 and 6, with several provisions. First, Notification 2022's challenges as a regulatory framework, alongside the development of Notification 2017, reflect a strict liability approach that is inconsistent with an international immunity framework. Under Article 15 of the CCA, prosecuted intermediaries are considered offenders but may be exempt from punishment if they demonstrate compliance with the notifications. Section 6 of Notification 2022 requires intermediaries to remove offensive content within 24 hours of receiving notice. Similarly, Section 8 allows authorities to issue takedown notices with varying deadlines (e.g., 24 hours, three days, or seven days), depending on the type of information; in both national security cases and individual requests, content must be removed within 24 hours.²⁵ These stringent timeframes and regulatory pressures reflect a strict liability regime's proactive monitoring obligations. Failure to comply exposes intermediaries to presumed liability under Article 15 of the CCA, contradicting the presumption of innocence guaranteed by Article 29 of the Thai Constitution 2017 (Section 9, Notification 2022). Furthermore, many Thai scholars, including Suksri,²⁶ Pimton,²⁷ and Wattanachiwakul,²⁸ have criticized Article

²⁵ILaw, **Announcement from the Ministry of Digital Economy and Society: Internet Service Providers Must Remove Unlawful Content within 24 Hours, Discontinuation of the Appeals Process** [Online], available URL: <https://ilaw.or.th/node/6322>, 2022 (November, 24).

²⁶Sawatree Suksri, **Law on Computer and Cyber Crimes**. Textbook and Teaching Material Project, Faculty of Law, Thammasat University, 2021, 470, 473.

²⁷Pimton, *Liability of Service Providers as Intermediaries*, 24.

²⁸Rapeeporn Wattanachiwakul, *op. cit.*, p. 22.

15 for defining penalties equivalent to those imposed on the primary offender, despite intermediaries functioning more akin to advocates, warranting a lesser penalty under Article 86 of the Thai Criminal Code. These obligations foster over-compliance and self-censorship, which disproportionately affect smaller platforms. Concerns articulated in the Memorandum of the Office of the Council of State highlight the financial and operational burdens of proactive monitoring, including high costs, risk of over-removal, and increased fees for citizens.²⁹

Second, judicial interpretations further amplify the chilling effect created by Thailand's strict liability framework. In *Prachatai*, the court held the intermediary liable despite its passive role in content hosting. Supreme Court Judgment No. 319/2560 (2017) remains one of the few Supreme Court decisions rendered under Section 15 of the CCA. Nevertheless, it does not strictly constitute a case of intermediary liability. As the Court expressly held, Matichon Online acted as a publisher by presenting news in its own name and exercising editorial control over the content. Therefore, the case falls squarely within the domain of publisher or editor liability, rather than liability for third-party content under a mere-conduit or hosting model. This doctrinal misalignment underscores the urgent need for clearer and more differentiated obligations under Section 15 of the CCA, particularly to distinguish intermediary functions from editorial activities, as well as to prevent the inappropriate extension of strict liability to genuine intermediaries. Wattanachiwakul³⁰ supports the view that editorial discretion could make intermediaries liable for content, even under the MCP. Thai judicial interpretations mirror aspects of Chinese jurisprudence; for instance, in *Wang v. Daqi and Tianya* (2008-2009), the court ruled that Tianya should have removed a specific post after either discovering it on its own or after being notified of its existence.³¹ This trend reflects Schauer's³² comparative harm principle,

²⁹Office of the Council of State, Memorandum of the Office of the Council of State accompanying the draft of the Computer-Related Offenses Act B.E. Report No. 919/2558, 2015, 2.

³⁰Rapeeporn Wattanachiwakul, op. cit.

³¹Qian Tao, "Intermediary Liability of Website Operators in Privacy Cases in China," *Masaryk University Journal of Law and Technology* 5, 1 (2011): 112.

³²Frederick Schauer, "Fear, Risk and the First Amendment: Unraveling the Chilling Effect," pp. 685-702.

which suggests that the cumulative costs of excessive speech suppression outweigh the risks posed by permitting controversial speech, highlighting the disproportionate impact of Thailand’s liability regime.

Despite the 2017 amendment to the CCA, strict liability remains a foundational concern. Scanlon’s³³ legitimacy framework asserts that restrictions on FOE must be justified under principles acceptable to all reasonable individuals, ensuring clear and predictable legal standards rather than fostering uncertainty. Similarly, Schauer highlights the chilling effect of vague regulations,³⁴ emphasizing the need for sufficient procedural safeguards to uphold legitimacy and proportionality.

However, Thailand’s regulatory approach continues to rely on ambiguous statutory terms, such as “collaborates in,” “gives consent to,” or “connives”—as mentioned in Section 5(1)(ข) of Notification 2022, the CCA of 2007, and its 2017 amendment—fostering considerable legal uncertainty. Conversely, language such as “not involved in” or “has no participation in determining or selecting the data or content,” found in Notification 2022, implies no editorial discretion by Internet intermediaries, which might assist in legal interpretation. However, without sufficient post-2017 case law, the extent of judicial deference to amendments remains uncertain.

2.1.2 Strict Liability’s Implications in Thailand

Strict liability in Thailand intermediary-liability framework presents several fundamental challenges. The most pressing issue is the chilling effect on FOE. By assigning liability based solely on the presence of illegal content, rather than intent or direct involvement, the law discourages robust public discourse. This approach aligns with Schauer’s³⁵ critique of vague regulations, which create incentives for over-compliance and self-censorship, as well as the *Prachatai* case, which showed that the Thai court does not differentiate between active participation in content dissemination and passive hosting, leading to a legal landscape where intermediaries

³³Thomas Scanlon, op. cit., pp. 204–226.

³⁴Frederick Schauer, op. cit., pp. 685–732.

³⁵Ibid., pp. 685–702.

remove content pre-emptively to mitigate risk. Therefore, the immunity framework should be applied in Thai law and adopted by court interpretation.³⁶

Despite amendments in 2017, Thailand's framework has failed to establish a clear presumption of non-liability; introducing explicit statutory protections that affirm non-liability for passive hosting would mitigate these risks and bring the law more closely in line with international best practices. This study argues that the notifications lack clarity regarding the timeframe within which Internet intermediaries must respond to illegal content once they know of it, either through self-detection or external direct user notice without authority interference.

Additionally, the wording of the CCA 2017 is problematic because service providers may be exempt from penalties if they can prove that they complied with notifications; nevertheless, the CCA does not explicitly state that they are absolved of liability. This discrepancy implies that Thai law continues to view intermediaries as fundamentally liable under all circumstances, highlighting the concept of strict liability in Thai law, whereby liability may be imposed regardless of intent or negligence. This reflects how Scanlon's³⁷ proportionality threshold is insufficient, as restrictions by a democratic state should be necessary, justified, and structured to minimize their impact on legitimate speech.

Thus, the current interpretation of the CCA reveals inconsistencies in the protection of the FOE, a fundamental right guaranteed in Article 34 of the Thai constitution and safeguarded under international law, including Article 19(3) of the International Covenant on Civil and Political Rights,³⁸ to which Thailand has been bound since 1996, and Article 19 of the Universal Declaration of Human Rights.³⁹ These inconsistencies ultimately weaken the legitimacy of Thailand's regulatory model.

³⁶Louise Timmermans, op. cit., p. 55; Baiyang Xiao, op. cit., p. 10.

³⁷Thomas Scanlon, op. cit., pp. 204–226.

³⁸Giancarlo F. Frosio, "Why Keep a Dog and Bark Yourself? From Intermediary Liability to Responsibility," *International Journal of Law and Information Technology* 26, 1 (2018): 12; Louise Timmermans. Op. cit., p. 8, 50.

³⁹Ibid., p. 8; Pattamon Anansaringkarn and Ric Neo, op. cit., p. 295.

Government enforcement trends may also substantially influence intermediary liability. Balkin conceptualizes algorithmic governance and technological infrastructure as the reliance on private platforms to indirectly enforce state censorship increases.⁴⁰ In Thailand, government agencies use intermediaries as *de facto* content regulators, particularly under *lèse-majesté* laws and the CCA. During the 2017 and 2020 pro-democracy movements, the Thai government threatened Facebook with criminal liability and platform shutdown unless it complied with takedown demands, providing a clear example of how social media platforms have been targeted by the Thai junta government to enforce laws and suppress FOE.⁴¹ Such state-driven pressure risks fostering discriminatory practices and a lack of transparency in the implementation of notice-and-takedown mechanisms.⁴² While the post-2020 period has coincided with the gradual consolidation of formally elected governments, there is little evidence of a fundamental relaxation in the enforcement logic governing sensitive political content. Although enforcement has become less overtly confrontational than during the junta period, the structural reliance on intermediaries to pre-emptively manage legal risk persists. This continuity continues to incentivize excessive compliance, particularly in the absence of an explicit prohibition on general monitoring obligations. As of 2026, a more restrained enforcement approach—one that adheres strictly to notification-based takedown procedures and conditions liability on actual knowledge—would better align with Xiao⁴³ who argued that legal frameworks should explicitly prohibit general monitoring obligations to ensure regulatory clarity. Without such protection, intermediaries may engage in excessive pre-emptive compliance, disproportionately affecting smaller platforms that are unable to meet stringent takedown demands.

The absence of judicial oversight in the takedown process, particularly regarding national security-related content, greatly exacerbates the risk of abuse. Provisions under Notification 2017, Section 5(1)(๗), and the current Notification 2022, Section 6(1), are problematic because they allow individuals to directly request

⁴⁰Jack M. Balkin, op. cit., p. 1153, 1179.

⁴¹Pattamon Anansaringkarn and Ric Neo, op. cit., p. 293.

⁴²Louise Timmermans, op. cit., p. 54.

⁴³Baiyang Xiao, op. cit., p. 1.

content removal without adequate safeguards or oversight. The absence of due process protections enables potential abuses of takedown mechanisms.

2.1.3 The Absence of Legitimate and Proportionate Privacy-Rights Protection in Thailand

Wattanachiwakul⁴⁴ has focused on national security, overlooking intermediaries' contractual and tort duties in privacy protection. The 2017 Thai Constitution guarantees privacy as a fundamental right under Article 32; however, no clear legal framework exists for intermediary liability in privacy-related matters. This gap enables potential abuse, inconsistent enforcement, and arbitrary censorship, thus increasing unpredictability for intermediaries.⁴⁵ It is also unclear how the Thai court should proceed with an infringement of privacy rights and whether the MCP would be applied. Meanwhile, Chinese scholars (e.g., Tao⁴⁶) have recognized the need to balance privacy rights with FOE in intermediary regulations. While the Thailand Personal Data Protection Act 2019, under Article 33, introduced the “right to be forgotten,” enabling rights-holders to request content takedowns, its framework lacks regulatory clarity (regarding tort liability's perspective) and judicial interpretation (regarding intermediary liability in privacy-related cases). This ambiguity underscores the urgent need for a well-defined legal framework to ensure legitimate and proportionate protection of privacy rights in Thailand.⁴⁷ Chinese law provides a specific tort framework for intermediary liability, as reflected in Article 1195 of the Civil Code of the People's Republic of China (PRC), which encompasses broader remedial measures, including deletion, blocking, or disconnection. This study proposes adopting a similar approach to enhance the clarity and scope of Thailand's intermediary obligations.

⁴⁴Rapeeporn Wattanachiwakul, op. cit., p. 9.

⁴⁵Pattamon Anansaringkarn and Ric Neo, op. cit, p. 290; Kate Klonick, op. cit., p. 1632; Guosong Shao, *Internet Law in China* (Kingston Upon Hull: Chandos Publishing, 2012), p. 56.

⁴⁶Qian Tao, “Intermediary Liability of Website Operators in Privacy Cases in China,” *Masaryk University Journal of Law and Technology* 5, 1 (2011): 105–118.

⁴⁷Sawatree Suksri, op. cit., pp. 488-494.

2.2 Lessons from China's Regulatory Framework

China's intermediary-liability framework adopts a dual approach: strict public law obligations prioritize national security, while private law integrates the MCP.

2.2.1 Liability Framework: MCP or Strict Liability?

Chinese public laws, particularly those concerning politically sensitive content, impose a strict liability model.⁴⁸ Laws such as the PRC Cybersecurity Law (Articles 12 and 47) and the PRC Regulation on Internet Information Services (Articles 15 and 16) impose onerous compliance burdens on intermediaries, demanding swift takedown of content deemed harmful to state security, secrecy, and national unification. This approach has led to a systemic chilling effect, curtailing online discourse and suppressing controversial viewpoints.⁴⁹ While Article 35 of the PRC Constitution (2018 Amendment) guarantees FOE, it is frequently subordinated to state security interests, leading to extrajudicial censorship measures.⁵⁰

China's cyber-paternalism prioritizes national security through stringent regulatory measures, reflecting its legal tradition of collectivism over individual rights. This justifies the government's reliance on notice-and-takedown measures to regulate online content. However, this article advocates for a different approach in Thailand, emphasizing individual rights and alignment with international standards.⁵¹ Specifically, it proposes adopting China's private-law model while rejecting strict liability, which risks state overreach and the suppression of democratic discourse. Shifting toward an immunity-based framework would reduce the burden on intermediaries and prevent their role as state censorship enforcers.

⁴⁸Louise Timmermans, op. cit., p. 31, 54, 60; Baiyang Xiao, op. cit., p. 5.

⁴⁹Ibid.

⁵⁰Louise Timmermans, op. cit., p. 54; Sabine A. Einwiller and Sora Kim, "How Online Content Providers Moderate User-generated Content to Prevent Harmful Online Communication: An Analysis of Policies and Their Implementation," **Policy and Internet** 12, 2 (2020): 184–206; Guosong Shao, op. cit., p. 50.

⁵¹Ibid., p. 54; Sabine A. Einwiller and Sora Kim, op. cit., p. 189.

The MCP is well established in Chinese tort law.⁵² Article 36 of the Tort Liability Law (now codified in the PRC Civil Code) stipulates that Internet users or network service providers bear tort liability for civil rights infringement.⁵³ Under this provision, an Internet user may request a notice-and-takedown action against privacy infringement (constituting a tort), while the network service provider must “take the necessary measures” upon being notified. If the provider fails to comply “in a timely manner,” it is considered jointly liable.⁵⁴ Furthermore, Articles 1194-1197 comprehensively reaffirm intermediary obligations,⁵⁵ balancing accountability with proportionality in addressing privacy infringements.

This framework creates a clear distinction between state-enforced censorship measures and private-law obligations, ensuring that privacy disputes remain within the civil law domain rather than being subject to broad government mandates.

2.2.2 The Timeframe for Takedown Obligations: Fixed or Case-By-Case?

Under Chinese law, the MCP requires intermediaries to act “expeditiously” to remove unlawful content after becoming aware of it, guided by the knowledge-based liability principle.⁵⁶ Article 1195 of the PRC Civil Code mandates that takedowns should occur in a “timely manner.” However, the law does not offer a precise definition of “timely,” leaving considerable discretion to the courts to assess each case based on its specific circumstances.

Judicial interpretations demonstrate the evolving expectations of the Chinese courts regarding intermediaries. In *Zhang v. Tianya* (2006), the courts imposed particularly stringent expectations, holding the intermediary liable for failing to remove defamatory posts that had garnered over 50,000 views within 72 hours.⁵⁷ In *Wang v. Daqi and Tianya* (2008-2009), courts adopted a more balanced approach, requiring

⁵²Baiyang Xiao, op. cit., p. 2.

⁵³Ibid., p. 4.

⁵⁴Guosong Shao, op. cit., p. 151.

⁵⁵Baiyang Xiao, op. cit., p. 2, 4.

⁵⁶Qian Tao, op. cit., p. 109.

⁵⁷Ibid., pp. 110–111.

valid notice before imposing a takedown obligation,⁵⁸ while recognizing platforms as gateways rather than publishers. However, in *Yin v. Baidu* (2009), the court introduced the concept of constructive knowledge, holding Baidu liable for publicizing infringing content even without formal notice, further expanding the scope of intermediary liability.⁵⁹ Constructive knowledge imposes a higher burden than traditional notice-and-takedown obligations but is considered a reasonable standard for intermediary liability. This approach is articulated in Article 1197 of the PRC Civil Code. Timmermans,⁶⁰ who has studied the European and international approaches, acknowledges that in a knowledge-based liability system for notice-and-takedown measures, the Internet intermediary shall not be held liable without knowledge or after promptly removing the flagged content once aware of it. Good-faith actions, such as voluntary proactive monitoring, should not undermine immunity. Accordingly, Xiao⁶¹ argues that even if diligent monitoring is unsuccessful, it should exempt intermediaries from liability.

2.2.3 Who Should Notify Internet Intermediaries of Their Takedown Obligations?

In China, public law imposes proactive monitoring obligations under a strict liability framework, requiring intermediaries to independently record and report infringing content to the authorities. However, it does not specify who has the right to notify intermediaries, as seen in Article 16 of the PRC Regulation on Internet Information Services and Article 47 of the PRC Cybersecurity Law. In contrast, private law adopts a more balanced and rights-oriented approach under the MCP. Article 1195 of the PRC Civil Code explicitly grants rights holders the authority to notify intermediaries about privacy infringement. This framework reflects the private nature of privacy disputes and prioritizes proportionality, ensuring that individuals can request direct actions from intermediaries.

⁵⁸Ibid., pp. 112–113.

⁵⁹Ibid.

⁶⁰Louise Timmermans, “op. cit., pp. 7, 27–28.; Constructive knowledge from the author point of view’s means that liability may arise where an intermediary ought reasonably to have known of the unlawful nature of the content, given its visibility, duration, or the intermediary’s degree of control over the platform in which it is widely recognized as a reasonable and proportionate burden.

⁶¹Baiyang Xiao, op. cit., p.14.

3. Balancing FOE With National Security and Privacy Rights: The Role of Intermediary-Liability Frameworks

3.1 A Proportionate Legal Framework for Balancing FOE with National Security and Privacy Rights

3.1.1 Liability Framework: MCP or Strict Liability?

Regarding national security, Thailand's intermediary-liability framework under the CCA and *lèse-majesté* laws enforces strict liability, shifting censorship responsibilities to intermediaries. This fosters collateral censorship, in which intermediaries over-remove content to avoid legal risks exacerbated by vague national security laws.⁶²

Anansaringkarn and Neo have criticized Article 14 of the CCA for its broad application to content affecting national security or causing public anxiety,⁶³ highlighting its potential for misuse as a censorship tool. Article 15 reinforces strict liability and fosters collateral censorship, as demonstrated in the *Prachatai* case. It is debatable whether the court held the platform liable solely for the presence of illegal content without properly assessing its monitoring obligations,⁶⁴ especially given *Prachatai*'s capacity and technological resources for monitoring illegal content—despite the testimony indicating the platform received 2,800–2,900 new messages daily, rendering full compliance impractical.⁶⁵ The *Prachatai* case underscores the imbalance between national security enforcement and FOE.

⁶²*Ibid.*, p. 10; Jack M. Balkin, “Old-school/New-school Speech Regulation,” *Harvard Law Review* 127 (2014): 2308–2309; Giancarlo F. Frosio, *op. cit.*, p. 13; Tyrell Haberkorn, “Dictatorship as Occupation in Thailand,” *The Journal of Legal Pluralism and Unofficial Law* 49, 3 (2017): 342.

⁶³Pattamon Anansaringkarn and Ric Neo, *op. cit.*, pp. 296–297.

⁶⁴Baiyang Xiao, *op. cit.*, pp. 1–16.

⁶⁵*Law*, *op. cit.*

Koltay⁶⁶ contends that imposing gatekeeper responsibilities on intermediaries to pre-emptively review all content undermines FOE. His critique echoes Scanlon's⁶⁷ proportionality framework, which argues that legal restrictions must be structured to avoid unnecessary infringement on fundamental rights. The same principle informs the Memorandum of the Office of the Council of State, which supports liability only when intermediaries possess knowledge of illegal content, thus balancing regulatory goals with operational realities. This rationale promotes a proportionate framework suited to evolving technological and democratic contexts.⁶⁸ Currently, the assumption of no liability for the Internet intermediary could lead to problematic interpretations of the CCA, even with notifications. Non-compliance with the 24-hour takedown requirement in Sections 6 and 8 of Notification 2022 is often interpreted as imposing strict liability compared to a case-by-case basis, especially considering that the technology and capacities of Internet intermediaries could lead to liability.

The CCA's strict liability framework imposes considerable burdens on intermediaries, necessitating reforms to address collateral censorship and align with Thailand's democratic trajectory. Adopting the MCP also offers a practical solution for reducing state overreach. Leyland⁶⁹ and Anansaringkarn and Neo⁷⁰ argue that Thailand's 2007 CCA and *lèse-majesté* laws have been deployed as political tools—introduced after the 2007 military junta and during the 2014 coup, respectively—to centralize military control, regulate dissent, and prioritize national security over individual rights. Thus, with Thailand's reinstatement of democratic elections in 2019, these laws have faced increasing criticism, underscoring the need for meaningful reform.

⁶⁶András Koltay, *New Media and Freedom of Expression: Rethinking the Constitutional Foundations of the Public Sphere* (Oxford: Hart Publishing, 2019), p. 224.

⁶⁷Thomas Scanlon, op. cit., pp. 204–226.

⁶⁸Office of the Council of State, Memorandum of the Office of the Council of State Accompanying the Draft of the Computer-Related Offences Act B.E. Report No. 257/2548, 2005, p. 15.

⁶⁹Peter Leyland, op. cit., pp. 134–135.

⁷⁰Pattamon Anansaringkarn and Ric Neo, op. cit., p. 292.

Regarding privacy rights, Thailand's regulatory framework suggests the adoption of a dual-track approach to content moderation, inspired by China's system.⁷¹ An MCP-based model limiting intermediary liability to instances of actual knowledge of unlawful content would better balance privacy rights and FOE while reducing arbitrary enforcement arising from vague legal provisions.

China's situation highlights the risks of unclear intermediary responsibilities without clear tort liability for notice-and-takedown regarding privacy rights, similar to the current situation in Thailand. This was demonstrated by *Yin v. Baidu* (2009), where ambiguities regarding monitoring obligations came to the forefront.⁷² Improved frameworks could enable rights-holders to enforce privacy claims through accessible, effective mechanisms that do not impose an undue burden and include the right to appeal. In addition, such frameworks would prevent the risk of courts extending public law interpretations into privacy rights matters.

Thus, I propose incorporating these principles into the Thailand Civil and Commercial Code or a specific statute to ensure efficient privacy rights protection. Intermediary liability should arise only if intermediaries (1) have actual or constructive knowledge of infringing content and (2) fail to act promptly. This approach mirrors China's tort liability framework and balances privacy protection with operational clarity.

3.1.2 The Timeframe for Takedown Obligations: Fixed or Case-By-Case?

Thailand's regulatory framework for takedown obligations mandates a fixed 24-hour period to remove illegal content under Notification 2022. However, as demonstrated in the *Prachatai* case, in which illegal content was not removed for 20 days after the platform was notified,⁷³ such strict deadlines may disproportionately burden smaller platforms, as they lack the resources to promptly remove content. Thus, platforms may pre-emptively remove lawful content and disable content-sharing functions to avoid liability. After the mentioned case, *Prachatai* disabled its user-opinion-sharing function to mitigate legal risks, thereby undermining FOE and

⁷¹Baiyang Xiao, op. cit., p. 1.

⁷²Qian Tao, op. cit., p. 113.

⁷³ILaw, op. cit.

hindering the platform's ability to compete in the market. This response aligns with Schauer's⁷⁴ chilling effect theory, which suggests that vague or inflexible language related to uncertainty and false legal requirements encourages over-compliance, limiting lawful speech.

Additionally, the knowledge-based liability framework, developed from Article 1197 of the PRC Civil Code⁷⁵ and Article 47 of the PRC Cyberspace Law, imposes liability upon the Internet intermediary once it becomes aware of illegal content and could be adopted in the Thai context. In the *Prachatai* case, Chiranuch Premchaiporn, the director of the popular independent and nonprofit Thai Internet newspaper, *Prachatai*, was charged under the 2007 CCA for failing to act quickly to remove a post that insulted Thailand's royal monarchy. The key issue in the case was whether the court-imposed liability was solely based on the presence of illegal content on the platform or whether the timeframe of 20 days was deemed sufficient to acquire relevant knowledge. The judgment did not specify whether this period was measured from the date the content was posted, receipt of notice, or another point in time. This ambiguity raises questions about the threshold for this timeframe.⁷⁶ Although a precise determination remains uncertain, a comparative analysis of Chinese jurisprudence suggests that technological capacity and intermediary obligations should inform a case-by-case assessment of this liability timeframe. In the *Prachatai* case, the court, rather than law enforcement, ordered the takedown, potentially reinforcing its authoritative nature.

Thus, China's case-by-case approach offers valuable insights into the Thai context. In *Zhang v. Tianya* (2006), Tianya was held liable for not removing infringing posts within 35 hours after a complaint, thus reflecting stringent monitoring obligations. However, in *Wang v. Tianya* (2008-2009), liability was limited to instances of self-discovery or notification, with no liability ascribed because the posts had already been deleted before the lawsuit. These developments highlight the advantages of

⁷⁴Frederick Schauer, op. cit., pp. 685–732.

⁷⁵Office of the Council of State, Memorandum of the Office of the Council of State Accompanying the Draft of the Computer-Related Offenses Act B.E. Report No. 257/2548, 2005.

⁷⁶Rapeeporn Wattanachiwakul, op. cit., pp. 23, 25–26.

the case-by-case framework in balancing intermediary obligations and fundamental rights.⁷⁷

3.1.3 Who Should Notify Internet Intermediaries of Their Takedown Obligations?

Regarding national security, takedown requests should originate from courts or authoritative bodies such as the police, rather than individuals. While individual notices expedite addressing sensitive content, they risk disproportionately curtailing FOE by transferring judicial discretion to private actors.⁷⁸ Without judicial oversight, intermediaries may remove content without adequately assessing their legal obligations.⁷⁹ Private actors are ill-suited to balancing FOE with competing values,⁸⁰ particularly in Thailand, where intermediaries may lack the cultural and legal understanding necessary to assess whether some specific content violates *lèse-majesté* or national security laws.

Thai regulations allow individuals to notify intermediaries of takedowns⁸¹ and risk granting intermediaries excessive discretion, thus leading to inconsistent standards and insufficient judicial intervention. Although this approach is suitable for straightforward legal cases, it imposes a tremendous burden on intermediaries in national security matters. A more balanced framework would require individuals to notify the police, who can assess and forward legitimate requests and ensure procedural safeguards. However, Pimton cautions that police involvement may also lead to abuse, with authorities potentially exploiting takedown mechanisms to bypass obligations.⁸² For instance, under Section 20 of the 2007 CCA and its 2017 amendment, competent officials with ministerial approval may petition the court to remove content.

However, regarding privacy rights, a court order for every takedown may be unnecessarily burdensome. In privacy-related situations, involving the courts in content removal may not be necessary. Instead, rights holders (as outlined in

⁷⁷Qian Tao, op. cit., pp. 110-113.

⁷⁸Aleksandra Kuczerawy, op. cit.

⁷⁹Marjorie Heins, op. cit., p. 329.

⁸⁰Louise Timmermans, op. cit., pp. 53-54.

⁸¹Pimton, op. cit., pp. 2-3, p. 48.

⁸²Ibid., pp. 48-49.

Article 1195 of the PRC Civil Code) or administrative authorities could be empowered to request takedowns, thus establishing a more streamlined process while protecting individuals' privacy rights.⁸³

3.2 A Proportionate Legal Framework for Supporting Technological Advancement

The Chinese case *Wang v. Daqi and Tianya* (2008-2009) underscores the importance of factoring in intermediaries' technological capabilities when determining their liability.⁸⁴ In the digital era, large companies, including Facebook, have adopted machine learning and filtering technologies to identify illegal and heterodox content.⁸⁵ The interpretation of the CCA and Notification 2022 should reflect these developments, which are consistent with the objectives articulated in the preamble of Notification 2022.

3.2.1 Liability Framework: MCP or Strict Liability?

According to Pimton and the Office of the Council of State,⁸⁶ the CCA and its accompanying notifications risk fostering self-censorship and incentivizing servers to relocate outside Thailand to avoid liability, thus deterring technological development and foreign investment. Therefore, granting intermediary immunity under a genuine MCP fosters innovation and enhances public-private collaboration.⁸⁷ Intermediary liability operates as a form of collaboration in which intermediaries equipped with advanced filtering technologies assist governments in their takedown efforts.⁸⁸ Compliance immunity enables collaboration without imposing undue liability.

⁸³Louise Timmermans, op. cit., pp. 29–55.

⁸⁴Qian Tao, op. cit., p. 113.

⁸⁵Sabine A. Einwiller and Sora Kim, op. cit., p. 197; Giancarlo F. Frosio, op. cit., pp. 14–15, p. 20; Tianxing He, op. cit., p. 78.

⁸⁶Pimton, op. cit., p. 3; Office of the Council of State. op. cit., p. 2.

⁸⁷Aleksandra Kuczerawy, op. cit.

⁸⁸Jack M. Balkin, op. cit., p. 2311.

The MCP offers a more equitable framework for intermediaries, particularly for smaller platforms. While larger platforms with sufficient resources can comply with monitoring obligations,⁸⁹ this may involve adopting new technology for filtering, thus eventually reducing costs. However, as observed in the *Prachatai* case, smaller platforms may be disadvantaged by a strict liability framework. Interestingly, *Prachatai* was forced to cancel its web board features, which began in July 2010 and promoted FOE by enabling users to share their opinions.⁹⁰ This worked against the creation of a free marketplace of ideas that should not be limited by states.⁹¹ According to Pimton,⁹² the application of Section 15 of the CCA 2007, including the *Prachatai* case, represents a burden on small-sized platforms, especially when the platform hosts a massive amount of content. Therefore, an MCP-based model would better suit platforms of various sizes, considering their resources, capacity, and costs, while also allowing them to compete in the market⁹³; this would align with Koltay's⁹⁴ argument that regulatory frameworks should consider varied business models and avoid stifling innovation. Moreover, excessive obligations contradict Mill's utility principle,⁹⁵ which advocates fostering long-term societal progress by protecting FOE and technological growth.

3.2.2 The Timeframe for Takedown Obligations: Fixed or Case-By-Case?

The timeframe for takedown obligations should be assessed on a case-by-case basis for both national security and privacy rights, with courts considering each company's technological advancement, capacity, and size. The disparity between large (e.g., Facebook, which employs automated moderation) and small (e.g., *Prachatai*, which relies on manual content review) platforms underscores the necessity of

⁸⁹Baiyang Xiao, op. cit., p. 15.

⁹⁰Law, op. cit.

⁹¹Andras Koltay, op. cit., p. 10.

⁹²Pimton, op. cit., p. 26.

⁹³Baiyang Xiao, op. cit., p. 15.

⁹⁴Andras Koltay, op. cit., pp. 233–234.

⁹⁵John Stuart Mill, *On Liberty, Utilitarianism, and Other Essays* (Oxford: Oxford University Press, 2015), p. 14.

flexible standards.⁹⁶ In *Wang v. Tianya*, the court ruled that liability should only apply when intermediaries receive proper notice or discover infringing content independently; thus, regulations should acknowledge intermediaries' technological limitations. Furthermore, Koltay⁹⁷ contends that while advancements in content moderation challenge intermediaries' classification as passive actors, mandating proactive monitoring without external notification remains both impractical and legally untenable. Accordingly, a rigid and fixed timeframe is inadequate, necessitating a more context-specific approach to establishing intermediary liability.

Automated filtering technology is often inadequate for filtering sensitive content, such as *lèse-majesté* posts. Algorithms can struggle to interpret nuanced or context-specific content, such as vague statements or wordplay, without proper legal or factual analyses.⁹⁸ Additionally, algorithms can fail to differentiate between lawful and unlawful content, thus leading to errors⁹⁹ that may create a chilling effect on FOE and contribute to transforming the Internet into a digital panopticon.¹⁰⁰ Furthermore, the technology supporting notice-and-takedown obligations should rely on Internet intermediaries' voluntary participation, rather than being compulsory under regulatory frameworks, as demonstrated in copyright law and filtering obligations in China.¹⁰¹ Accordingly, beyond the sensitivity and nature of flagged content, such regulations should also consider the size and capacity of the company in question, such as its number of monthly active users.¹⁰²

⁹⁶ILaw, op. cit.,

⁹⁷Andras Koltay, op. cit., p. 95.

⁹⁸ILaw, op. cit.

⁹⁹Louise Timmermans, op. cit., p. 22.

¹⁰⁰Baiyang Xiao, op. cit., pp. 1, 8, 10.

¹⁰¹Tianxing He, op. cit., pp. 71–94.

¹⁰²Baiyang Xiao, op. cit., p. 15.

4. Conclusion and Proposals for Reform

This study assessed Thailand's notice-and-takedown framework and examined its legitimacy and proportionality using comparative insights. The findings underscore the need for reforms to balance national security, FOE, and privacy rights. Aligned with the MCP, this study proposes a context-specific interpretation of the MCP tailored to Thailand's legal environment, where freedom of expression remains particularly sensitive to over-enforcement. In this sense, the MCP should function as a normative safeguard against the indirect delegation of censorship powers to private actors. Under this approach, an intermediary whose role is confined to the neutral transmission or hosting of third-party content—without initiating, selecting, modifying, or exercising editorial judgment—should not be liable by default. Liability should arise only where legally cognizable knowledge of unlawfulness has been established through procedurally legitimate mechanisms. On this basis, this study advances the following policy initiatives:

(1) Institutionalizing a case-specific takedown mechanism for national security and a clear privacy framework to ensure safeguards: Thailand should adopt a case-by-case approach to takedowns rather than a rigid liability framework, incorporating constructive knowledge as a standard for intermediary liability, as opposed to the *de facto* assumption of liability.¹⁰³

Regarding national security, identifying *lèse-majesté* content is a legitimate state interest. However, the Thai legal system's approach to intermediary liability must balance this with FOE. Balkin¹⁰⁴ discusses how governments use both incentives and coercive measures to regulate intermediaries, offering immunity in exchange for compliance. Thailand's reliance on takedown measures rather than counter speech strategies raises concerns about their chilling effect on public discourse. Adopting a

¹⁰³Ibid., p. 14; Louise Timmermans. op. cit., p. 55.

¹⁰⁴Jack M. Balkin, op. cit., p. 2299.

case-by-case approach, rather than blanket liability, aligns with Scanlon's¹⁰⁵ proportionality theory and Mill's¹⁰⁶ emphasis on open debate as a mechanism for truth-seeking.¹⁰⁷ Thailand's 24-hour timeframe for takedowns appears overly stringent. Similarly, Gillespie¹⁰⁸ has criticized the United Kingdom's two-day timeframe for addressing terrorist content, highlighting its impracticality. Thailand's shorter time frame raises similar concerns, particularly given the comparatively low sensitivity of the content involved.

A case-by-case approach provides greater flexibility for courts to assess content sensitivity and its impact on national security, thereby serving as a compromise for government control. The *Prachatai* case demonstrates this, as the court applied a case-specific assessment, deeming 1-11 days a sufficient timeframe, but stating that 20 days was excessive.¹⁰⁹

Moreover, Article 15 of the CCA should explicitly state, “the service provider is not liable,” akin to the EU Directive 2000/31/EC: “Member States shall ensure that the service provider is not liable,” rather than using vague wording in which strict liability is assumed (“Any service provider who collaborates in, gives consent to or connives shall be liable”). According to the historical development of the CCA, service providers who “become aware of” unlawful acts in computer systems under their control and “fail to promptly remove” the computer data—specifically at the earliest opportunity upon gaining knowledge and the ability to do so—shall be subject to criminal liability. It appears that knowledge-based liability was initially clearly adopted in the CCA; however, during the review process of the National Legislative Assembly, amendments were made to reflect the intention of holding service providers accountable for monitoring obligations, in contrast to the MCP proposed by the

¹⁰⁵Thomas Scanlon, op. cit., pp .209, 224.

¹⁰⁶John Stuart Mill, op. cit., p. 19.

¹⁰⁷Jack M. Balkin, op. cit., p. 4.

¹⁰⁸Tarleton Gillespie, **Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions that Shape Social Media** (New Haven: Yale University Press, 2018), p. 37.

¹⁰⁹Rapeeporn Wattanachiwakul, op. cit., pp. 25–26.

present study. Consequently, the wording of the CCA (2007) changed from “become aware of” to “intentionally support or consent to,”¹¹⁰ as well as “collaborates in, gives consent to or connives,” in the CCA’s latest amendment (2017). Thus, because Internet intermediaries have not directly committed a crime in such cases, this study proposes adopting new wording consistent with knowledge-based liability, thereby lessening the obligation for Internet intermediaries, especially smaller platforms.

Such knowledge-based liability should account for the size and technological capacity of service providers. Under a refined knowledge-based liability model, platforms such as *Prachatai* may not have been held liable.

Upon the enactment of the notifications, the Thai regulatory framework might conditionally reflect a knowledge-based approach based on different types of intermediaries, which would impose different editorial discretion on infringed content. This is referred to as the partially knowledge-based hybrid model, but the law should explicitly state that intermediaries are not liable in the CCA (the parent law), thus ensuring greater legal certainty and a balanced approach between FOE and national security, as well as genuinely reflecting the MCP and the elimination of strict liability by the Thai state.

From the perspective of privacy rights, clear regulations on intermediary liability are essential to address existing legal uncertainty in Thailand. While privacy is primarily a private-law matter and less sensitive than national security, the absence of specific statutory provisions results in inconsistent enforcement. Therefore, Thailand should adopt explicit rules stating that “a service provider is not liable unless it knowingly facilitates illegal content,” or at the very least, “A network user or network service provider who infringes upon the civil right or interest of another person through their network shall assume tort liability” (in line with Chinese law’s wording), rather than relying on general tort law, as the broad and unpredictable application of Article 420 of the CCA in privacy-related takedown cases has made its use problematic. Judicial interpretations of general tort law have historically led to inconsistencies, particularly

¹¹⁰Pimton, op. cit., pp. 22-23; Office of the Council of State, op. cit., p. 15.

regarding the scope of liability and the recognition of mental damage in privacy violations. Similar challenges have been observed in China, where courts struggled to apply tort liability to intermediary obligations before clearer statutory frameworks were introduced. Furthermore, a 2023 Thai study notes the inadequacy of Article 420 in protecting privacy rights, which may be caused by its vague scope, thus making it inappropriate for governing notice-and-takedown procedures.¹¹¹

(2) *Judicial oversight requirement for national security aspect:* Pimton highlights that a lack of judicial oversight in takedown processes, leaving discretion entirely to Internet intermediaries, can lead to abuse.¹¹² Furthermore, even when the content is deemed illegal, such a determination should rest with the courts. Judicial oversight—or, at the very least, police involvement as an authority in national security-related takedowns—is essential for ensuring fairness, proportionality, and legitimacy. This is particularly important for the protection of individual rights (including FOE), which fall primarily under the judiciary’s purview. Concurrently, individual rights holders (including administrative authorities) should retain the ability to issue notices for privacy-related obligations.¹¹³ However, an Internet intermediary should play a role in ensuring legally valid notices.

Upon enactment of notifications, individuals may report illegal content to the police, who can then investigate and initiate takedown procedures. However, whether these reporting mechanisms can sufficiently safeguard against abuse remains controversial. Relying solely on police decisions risks over-enforcement or selective enforcement, as police may lack the expertise to evaluate whether the content

¹¹¹Methinee Suwannakit, *The Protection of Privacy and Private Information in the Digital Age: A Comparative Study of English and Thai law Applying to Individual Media Users* (University of Glasgow, 2023), pp. 5, 176, 180, 185.

¹¹²Pimton, op. cit., pp. 31, 43.

¹¹³Jack M. Balkin, op. cit., pp. 47–48; Aleksandra Kuczerawy, op. cit.; Louise Timmermans, op. cit., p. 29.

genuinely violates national security laws. Thus, a clearer role for judicial oversight would mitigate these concerns by ensuring due process and legitimacy.

A clear application of the MCP would modernize Thailand's legal framework to align with global regulatory trends. This would protect intermediaries from uncertainty regarding the various local regulations. This follows Schauer's¹¹⁴ theory by balancing national security, privacy, and intermediary liability. By integrating a knowledge-based liability model, judicial oversight, and clear privacy protections, this reform would enhance fairness, efficiency, and compliance while safeguarding constitutional protections for FOE. Harmonizing with international frameworks, including the EU and Chinese approaches, would ensure regulatory coherence and support cross-jurisdictional interoperability.

This study contributes to the global discourse on intermediary liability by demonstrating how the MCP can function as a constitutional safeguard against indirect state censorship and as a mechanism for protecting freedom of expression in digital environments. Although this study tailors its analyses to Thailand's legal and political context, the findings nevertheless reconceptualize the MCP beyond a purely technical and doctrinal definition, thereby providing scope for novel applications of the MCP to international contexts. This is further illustrated in this study's comparative analysis with China, whereby China's laws were used as an example contributing to the overall recommendations for Thailand. However, future comparative research must consider and accommodate differences in political and legal traditions, particularly regarding immunity for Internet intermediaries within evolving technological infrastructures. As Thailand shifts toward reformation under a uniform liberal-democratic jurisdiction, adopting such policy-driven reforms would position the nation as a leader in equitable and forward-looking digital governance.

Funding: This work was supported by the Article 112 Project at the Justice in Southeast Asia Lab, University of Wisconsin–Madison (the initial abstract and presentation were submitted to the funding organization and are available on its website).

¹¹⁴Frederick Schauer, *op. cit.*, p. 721.

Declaration of AI Assistance:

In the preparation of this study, AI tools were employed in a limited and supportive capacity. First, AI was used primarily for grammar proofreading, as well as for suggestions relating to word choice, sentence structure, and overall clarity. Second, AI tools were utilized to provide suggestions on the logical organization, content structure, and conceptual framework of the paper, thereby enhancing the author's ideas. All feedback generated by the AI tools was critically reviewed and assessed for accuracy and appropriateness by the author.

Bibliography

- Anansaringkarn, Pattamon, and Ric Neo. “How Can State Regulations over the Online Sphere Continue to Respect the Freedom of Expression? A Case Study of Contemporary ‘Fake News’ Regulations in Thailand.” **Information and Communications Technology Law** 30, 3 (2021): 283–303.
- Balkin, Jack M. “Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society.” **New York University Law Review** 79, 1 (2004): 1-55
- _____. “Old-school/New-school Speech Regulation.” **Harvard Law Review** 127, 8 (2014): 2296–2342.
- Einwiller, Sabine A., and Sora Kim. “How Online Content Providers Moderate User-generated Content to Prevent Harmful Online Communication: An Analysis of Policies and Their Implementation.” **Policy and Internet** 12, 2 (2020): 184–206.
- Frosio, Giancarlo F. “Why Keep a Dog and Bark Yourself? From Intermediary Liability to Responsibility.” **International Journal of Law and Information Technology** 26, 1 (2018): 1–33.
- Gillespie, Tarleton. **Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions that Shape Social Media**. New Haven, CT: Yale University Press, 2018.
- Haberkorn, Tyrell. “Dictatorship as Occupation in Thailand.” **The Journal of Legal Pluralism and Unofficial Law** 49, 3 (2017): 338–352.
- He, Tianxing. “Online Content Platforms, Copyright Decision-making Algorithms and Fundamental Rights Protection in China.” **Law, Innovation and Technology** 141 (2022): 71–94.
- Heins, Marjorie. “The Brave New World of Social Media Censorship.” **Harvard Law Review Forum** 127, 8 (2014): 325–330.
- ILaw. **Announcement from the Ministry of Digital Economy and Society: Internet Service Providers Must Remove Unlawful Content within 24 Hours, Discontinuation of the Appeals Process** [Online]. Available URL: <https://ilaw.or.th/node/6322>, 2022 (November, 24).

- _____. **hiranuch Premchaiporn: Director of Prachatai** [Online]. Available URL: <https://www.ilaw.or.th/articles/case/23450>, 2016 (December, 2).
- International Commission of Jurists. **Dictating the Internet: Curtailing Free Expression and Information Online in Thailand**. April 2021.
- Klonick, Kate. “The New Governors: The People, Rules, and Processes Governing Online Speech.” **Harvard Law Review** 131, 6 (2018): 1598–1670.
- Koltay, András. **New Media and Freedom of Expression: Rethinking the Constitutional Foundations of the Public Sphere**. Oxford: Hart Publishing, 2019.
- Kuczerawy, Aleksandra. “From ‘Notice and Take Down’ to ‘Notice and Stay Down’: Risks and Safeguards for Freedom of Expression.” in **The Oxford Handbook of Intermediary Liability Online**, edited by Giancarlo F. Frosio. Oxford: Oxford University Press, 2019.
- La Rue, Frank. **Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression** [Online]. Available URL: <https://digitallibrary.un.org/record/706200?v=pdf>, 2011 (May, 27).
- Leyland, Peter. “The Struggle for Freedom of Expression in Thailand: Media Moguls, the King, Citizen Politics and the Law.” **Journal of Media Law** 2, 1 (2010): 115–137.
- Mill, John Stuart. **On Liberty, Utilitarianism, and Other Essays**. Oxford: Oxford University Press, 2015).
- Nizam, Fuad. “MCMC to Take Legal Action Against Meta over Noncooperation to Remove Undesirable Contents from its Platform.” **New Strait** [Online]. Available URL: <https://www.nst.com.my/news/crime-courts/2023/06/923358/mcmc-take-legal-action-against-meta-over-non-cooperation-remove>, 2023 (June, 23)
- Office of the Council of State. **Memorandum of the Office of the Council of State Accompanying the Draft of the Computer-Related Offenses Act B.E. Report No. 257/2548, 2005**.
- Office of the Council of State. **Memorandum of the Office of the Council of State Accompanying the Draft of the Computer-Related Offenses Act B.E. Report No. 919/2558, 2015**.

- Pimton, C. **Liability of Service Providers as Intermediaries: Notification of Computer Data Suspension and Removal from Computer Systems**. Bangkok: Chulalongkorn University, 2018.
- Prachatai. **Netizen Network: Summary of Movements Internet Case and the Liability of the Intermediary “Director of Prachatai”** [Online]. Available URL: https://prachatai.com/journal/2012/04/40258?__cf_chl_rt_tk=ROeVBqo5Fo9moenYiJAeBh09Bs2_hF0Sn08NHP5_SUQ-1700208807-0-gaNycGzNEtA, 2012 (April, 27).
- Royal Thai Government. **Notification of the Ministry of Digital Economy and Society Re: Procedures for Notification, Suspension of Dissemination of Computer Data, and removal of computer data from computer systems**, 22 July 2017.
- Royal Thai Government. **Notification of the Ministry of Digital Economy and Society Re: Procedures for notification, suspension of dissemination of computer data, and removal of computer data from computer systems**, 26 October 2022.
- Scanlon, Thomas. “A Theory of Freedom of Expression.” **Philosophy and Public Affairs** 1, 2 (1972): 204–226.
- Schauer, Frederick. “Fear, Risk and the First Amendment: Unraveling the Chilling Effect.” **Boston University Law Review** 58 (1978): 685–732.
- Shao, Guosong. **Internet Law in China**. Kingston Upon Hull: Chandos Publishing, 2012.
- Southeast Asian Press Alliance. **SEAPA Submission to Study on Social Media, Search, and Freedom of Expression** [Online]. Available URL: <https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/ContentRegulation/Seapa.pdf>, n.d.
- Suksri, S. **Law on Computer and Cyber Crimes. Textbook and Teaching Material Project**. Bangkok: Faculty of Law, Thammasat University, 2021.
- Suwannakit, Methinee. **The Protection of Privacy and Private Information in the Digital Age: A Comparative Study of English and Thai Law Applying to Individual Media Users**. Glasgow: University of Glasgow, 2023.
- Tao, Qian. “Intermediary liability of website operators in privacy cases in China.” **Masaryk University Journal of Law and Technology** 51 (2011): 105–118.
- Timmermans, Louise. “The Role of Internet Intermediaries in the Protection of Freedom of Expression and Personal Data: Human Rights in a Digital Age.” Master’s thesis, University of Montpellier, 2017.

- TLHR. **January 2024: A Total of 1,947 People Has Been Politically Prosecuted Resulting in 1,268 Lawsuits** [Online]. Available URL: <https://tlhr2014.com/en/archives/64902>, 2024 (February, 19).
- Tortermvasana, Komsan and Online Reporters. **Facebook Faces Immediate Shutdown Threat** [Online]. Available URL: <https://www.bangkokpost.com/thailand/politics/1250114/facebook-faces-immediate-shutdown-threat>, 2017 (May, 16).
- _____. **Statistics of Lèse Majesté Cases with Court Rulings in Thailand** [Online]. Available URL: <https://tlhr2014.com/archives/46268>, 2022 (March, 28).
- Van Hoecke, Mark. **Epistemology and Methodology of Comparative Law**. London: Bloomsbury Publishing, 2004.
- Wattanachiwakul, Rapeeporn. **Liability Issues of Internet Service Providers as “Intermediaries” under the Computer-Related Crime Act B.E., 2550**. Judicial Official Development Institute, Office of the Judiciary, 2014.
- Xiao, Baiyang. “Making the Private Public: Regulating Content Moderation under Chinese Law.” **Computer Law and Security Review** 51 (2023): 1–16.