



Consumer Privacy and Data Tracking in the Digital Economy: Legal Frameworks and Future Challenges in Indonesia and Thailand

Agustianto^{1✉}, Nipon Sohheng², Lu Sudirman³, Triana Dewi Seroja⁴, Nurlailiy⁵

^{1,3,4,5} Faculty of Law, Universitas Internasional Batam, Indonesia

² Faculty of Political Science, Ramkhamhaeng University, Thailand

Corresponding: agustianto.lec@uib.ac.id

Article Process Abstract

Submitted:
2025-02-17

Reviewed:
2025-03-18

Accepted:
2025-09-20

Published:
2025-09-29

This study analyzes the adequacy of consumer data protection frameworks in Indonesia and Thailand in addressing privacy threats posed by advanced tracking technologies through the lens of human rights. Using normative legal research methodology supported by a comparative approach, this study examines how both countries' legal frameworks govern data tracking technologies in their rapidly digitalizing economies. The analysis reveals significant weaknesses in both Indonesia's Personal Data Protection Law and Thailand's Personal Data Protection Act, particularly in their classification frameworks for advanced tracking technologies that combine machine learning algorithms with cross-device behavioral pattern analysis. While Thailand demonstrates superior protection against consent bundling, both countries lack comprehensive data classification systems and adequate mechanisms to address privacy threats from sophisticated tracking technologies. This study proposes a model of legal development to enhance consumer data protection in both jurisdictions, emphasizing the need for immediate reforms to protect privacy rights in the face of evolving digital tracking capabilities. The findings underscore the urgency for both countries to strengthen their legal frameworks to balance economic growth with fundamental human rights in the digital economy. The insights that this study provides contribute to the growing literature around consumer privacy, while also highlighting practical implications for Indonesia and Thailand, particularly regarding lack of data classification as a significant legal gap that both countries need to tackle.

Keywords: Data governance; Data-Based Tracking; Digital Economy; Human Rights; Law Reform; Indonesia; Thailand

I. Introduction

The development of information and communication technology through digital transformation has fundamentally transformed the global economic landscape¹, driving societies around the world deeper into the era of digital economy². In digital economy, data becomes a valuable asset,³ as it plays a key role in helping businesses scale their operations and expand their reach.⁴ Data can now be utilized by businesses in tracking consumer behavior through relevant data and its analysis, which can significantly help marketing strategies and campaigns in digital spaces.⁵ This allows for a high level of personalization to tailor to the specific needs of each consumer, making their products and services more relevant and interesting.⁶ On the purely digital and technical side, the developers behind digital technologies that make this a possibility also utilize data to improve their services, through the aspect of performance optimization and even fraud detection for security purposes.⁷ From this perspective, users are also naturally viewed as consumers, as they are actively using the digital services and features provided in a digital platform.⁸ However, this practice often involves data collection with unclear consent forms, and even breaches of consumer privacy rights,⁹ ultimately affecting their autonomy in decision making.

Ideally, legal frameworks in the digital era must be able to ensure the protection privacy rights¹⁰ and freedom of consumers in making their own decisions, facilitated with a transparent information system regarding data tracking¹¹. However, this is often not the case in practice, and is even not extensively analyzed in countries with immense economic growth potentials, like Indonesia and Thailand.¹² Despite having enacted Law No. 27 of 2022 on Personal Data Protection and Personal Data Protection Act respectively, it is still quite unclear where Indonesia and Thailand stand on the issue of data tracking through technologies like cookies or caches. The lack

¹ Olesia Suntsova, "Digital Transformation of the Global Economy: Challenges and Opportunities," *Financial and Credit Systems: Prospects for Development* 3, no. 14 (September 2024): 10–87, <https://doi.org/10.26565/2786-4995-2024-3-08>.

² Waleed K Al-Zoubi, "Economic Development in the Digital Economy: A Bibliometric Review," *Economies* 12, no. 3 (2024): 1–28, <https://doi.org/10.3390/economies12030053>.

³ Tao Xu et al., "From Data to Data Asset: Conceptual Evolution and Strategic Imperatives in the Digital Economy Era," *Asia Pacific Journal of Innovation and Entrepreneurship* 18, no. 1 (January 2024): 2–20, <https://doi.org/10.1108/APJIE-10-2023-0195>.

⁴ Ariana Delhi and Apriani Sijabat, "The Role of Technology Adoption in Scaling Startuppreneur Business Models in the Digital Economy," *Startuppreneur Business Digital (SABDA Journal)* 3, no. 2 (October 2024): 141–47, <https://doi.org/10.33050/sabda.v3i2.631>.

⁵ Ahmad Al Adwan et al., "Data Analytics in Digital Marketing for Tracking the Effectiveness of Campaigns and Inform Strategy," *International Journal of Data and Network Science* 7, no. 2 (2023): 563–74, <https://doi.org/10.5267/j.ijdns.2023.3.015>.

⁶ Anne-Sophie Riegger et al., "Technology-Enabled Personalization in Retail Stores: Understanding Drivers and Barriers," *Journal of Business Research* 123 (2021): 140–55, <https://doi.org/https://doi.org/10.1016/j.jbusres.2020.09.039>; Lu Sudirman et al., "BEYOND LIKES AND FOLLOWS: Navigating Consumer Trust and IPR-Related Risks in Influencer Marketing," *Jurisdictie: Jurnal Hukum Dan Syariah* 15, no. 2 (January 2025): 245–73, <https://doi.org/10.18860/j.v15i2.28054>.

⁷ Kyungmin Sim, Honyeong Heo, and Haehyun Cho, "Combating Web Tracking: Analyzing Web Tracking Technologies for User Privacy," *Future Internet*, 2024, <https://doi.org/10.3390/fi16100363>.

⁸ Bakyt Tolegenov et al., "Digital Transparency and Consumer Awareness: Digital Platforms for Educating Consumers about Product Origins and Sustainability," *AL-MUZARA'AH* 12, no. 2 (December 2024): 277–87, <https://doi.org/10.29244/jam.12.2.277-287>.

⁹ Cedric Deslandes Whitney and Justin Norman, "Real Risks of Fake Data: Synthetic Data, Diversity-Washing and Consent Circumvention," in *The 2024 ACM Conference on Fairness, Accountability, and Transparency* (New York, NY, USA: ACM, 2024), 1733–44, <https://doi.org/10.1145/3630106.3659002>.

¹⁰ Brahmantyo Suryo Satwiko, "Privacy and Data Protection: Indonesian Legal Framework," *Corporate and Trade Law Review* 1, no. 2 (2021): 98–118, <https://doi.org/10.21632/ctlr.1.2.98-118>.

¹¹ Jewel Gausman et al., "Validation of a Measure to Assess Decision-Making Autonomy in Family Planning Services in Three Low- and Middle-Income Countries: The Family Planning Autonomous Decision-Making Scale (FP-ADM)," *PLoS ONE* 18, no. 11 (2023): 1–17, <https://doi.org/10.1371/journal.pone.0293586>.

¹² Muhammad Rizal and Erika Vivin Setyoningsih, "Perlindungan Konsumen Dalam Pemanfaatan Big Data Oleh Pelaku Bisnis Di Indonesia: Tinjauan Terhadap Regulasi Dan Implementasi Praktik Bisnis," *Jurnal Penegakan Hukum Dan Keadilan* 4, no. 1 (2023): 75–85; Panchapawn Chatsuwana et al., "Personal Data Protection Compliance Assessment: A Privacy Policy Scoring Approach and Empirical Evidence from Thailand's SMEs," *Heliyon* 9, no. 10 (2023): 1–30, <https://doi.org/https://doi.org/10.1016/j.heliyon.2023.e20648>.

of understanding regarding these tracking technologies in the general public makes this an even more urgent issue to be analyzed. These gaps are what must be properly and perhaps even exhaustively addressed as both Indonesia and Thailand are going deeper into the era of digital economy with the continued rise of widespread digital technology adaptation and all of their benefits to the economy.

Indonesia and Thailand are key players in Southeast Asia's economic growth, with Indonesia having the biggest GDP and Thailand coming in second.¹³ Both countries are also members of ASEAN, as the uniting geopolitical power in the region. ASEAN also acts as a platform for collaboration between its members. With the continued rise of economic growth in the digital era, both Indonesia and Thailand cannot afford to lose momentum, due to legal issues that could stifle the growth of their digital economies. Therefore, assessing how these two countries design their data protection mechanisms in the face of widespread use of data tracking technologies is important in ensuring that both Indonesia and Thailand can balance the need for economic growth with the right to privacy of digital technology users. The two legal frameworks mentioned previously, Indonesia's PDP Law and Thailand's PDPA, are the main focus of this study's normative analysis.

Most importantly, it is imperative to firmly address the urgency behind this legal issue. With the rise of technologies like AI and other machine learning processes,¹⁴ businesses and digital system providers can even predict what consumers are going to think or want.¹⁵ While this can be easily labeled as increased convenience, it can ultimately impact people's thinking patterns, particularly their consumption behavior,¹⁶ and ultimately questioning what makes up their perspectives of the world, along with their perceptions of autonomy.¹⁷ It is also easy to get caught up in the deeper, perhaps philosophical issues of this discourse. However, through the lens of human rights, legal analysis regarding this issue can be analyzed with better clarity and focus, to ultimately discuss what kind of legal compliance is needed to strike the balance between business accelerations and consumer's right to privacy, along with their right to make their own decisions.

The discourse of consumer data protection is a rather contentious legal academic topic, with research such as the ones conducted by Orla Lynskey (2023)¹⁸ and Maja Brkan (2019),¹⁹ stating that it is indeed a field marked by irreconcilable tensions between regulatory ambition and practical feasibility, where expansive legal frameworks risk diluting compliance efficacy while creating jurisprudential ambiguities. The former critiques the GDPR's near-universal application as a "law of everything", that burdens individuals and strains enforcement capacity. The latter identifies structural contradictions in EU frameworks, underscoring broad interpretations of privacy and data protection rights that clash with operational realities. Another study, conducted by Joanna Strycharz et al (2019), focuses specifically on cookies, which is a type

¹³ Lilies Setiartiti and Fitri Rahmadani, "Determinant of Economic Growth in ASEAN Countries (Indonesia, Thailand, Malaysia, Singapura, Philippines) 2010-2019," *Journal of Economics Research and Social Sciences* 7, no. 2 (2023): 253-64, <https://doi.org/10.18196/jerss.v7i2.19551>.

¹⁴ Emiliya Febriyani, Elza Syarief, and Triana Dewi Seroja, "Pemanfaatan Artificial Intelligence Dalam Deteksi Dan Pencegahan Tindak Pidana Pencucian Uang: Potensi Dan Tantangan Hukum?," *Jurnal Magister Hukum Udayana (Udayana Master Law Journal)* 13, no. 4 (2024): 877-98, <https://doi.org/10.24843/JMHU.2024.v13.i04.p10>.

¹⁵ Alessandro Mantelero, "The Future of Consumer Data Protection in the E.U. Re-Thinking the 'Notice and Consent' Paradigm in the New Era of Predictive Analytics," *Computer Law & Security Review* 30, no. 6 (2014): 643-60, <https://doi.org/https://doi.org/10.1016/j.clsr.2014.09.004>.

¹⁶ Muhammad Bilal et al., "Artificial Intelligence Is the Magic Wand Making Customer-Centric a Reality! An Investigation into the Relationship between Consumer Purchase Intention and Consumer Engagement through Affective Attachment," *Journal of Retailing and Consumer Services* 77 (2024): 1-11, <https://doi.org/https://doi.org/10.1016/j.jretconser.2023.103674>.

¹⁷ Michael Gerlich, "AI Tools in Society: Impacts on Cognitive Offloading and the Future of Critical Thinking," *Societies* 15, no. 1 (2025): 1-28, <https://doi.org/10.3390/soc15010006>.

¹⁸ Orla Lynskey, "Complete and Effective Data Protection," *Current Legal Problems* 76, no. 1 (November 2023): 297-344, <https://doi.org/10.1093/clp/cuad009>.

¹⁹ Maja Brkan, "The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way Through the Maze of the CJEU's Constitutional Reasoning," *German Law Journal* 20, no. 6 (2019): 864-83, <https://doi.org/DOI:10.1017/glj.2019.66>.

of data that is used for data analytics.²⁰ Cookies support advanced tracking, which according to the study, is a serious threat to privacy rights. The study also states that there needs to be a significant improvement in legal and technical knowledge to even understand the risks associated with this form of data tracking, indicating the serious commitment required.

In Indonesia, data protection has also been an issue that is often brought up in the academic sphere. One study, carried out by Masitoh Indriani and Annida Aqiila Putri (2023),²¹ indicated that the main issue behind data protection is how the data is used in the utilization digital services. The study notes that consent remains the key issue in this discourse is consent, which plays a very important role in the protection of data privacy in many cases of data collection and processing purposes, including data tracking for marketing purposes. Unfortunately, this has not been properly addressed by the Indonesian legal framework responsible for data protection. This is also the case with Thailand, as underscored by a study conducted by Chanchai Phonthanukitithaworn and Carmine Sellitto (2022).²² Even worse, some users in Thailand are actually willing to give up their personal data for monetary rewards, while also not being sure about the perceived risks associated with such act. This paradox shows that while regulation plays a key role in setting the standard for data protection, it might need to also facilitate the prevention of direct personal data purchases.

Despite the vast literatures, the discourse of consumer data protection in the context of data tracking technologies, has not been fully explored through the lens of human rights, particularly in the face of advanced tracking technologies. With the utilization of AI and other computing technologies that can accelerate and improve tracking technologies, there is a significant risk that data privacy concerns could get even more invasive, making it even more urgent to analyze this discourse extensively. This gap in the literature is what this study is aiming to fill, by scrutinizing the relevant legal frameworks in Indonesia and Thailand in a comparative manner. Furthermore, this study is also equipped with more novel elements in the analysis, as it does not only compare the existing Indonesian and Thai frameworks, but also analyze how the gaps that the two legal systems have are faring up to the growing risks of privacy concerns around data tracking technologies, and ultimately how they can be improved in future legal developments. Although the analysis of this research is not equipped with empirical evidence and is limited by legal normative boundaries, it nevertheless provides a novel angle of analysis on consumer data protection through the human rights lens, while carefully assessing its intersection with the domain of data protection in the context of advanced tracking technologies in Indonesia and Thailand. This analysis is important in providing a clearer picture of the significant threats that consumers face in the ever-so-digitalized world and could potentially be beneficial for the development of literature, which could serve as possible considerations in future policy development.

II. Research Problems

The article focuses on examining the boundaries of data tracking technologies in the digital economy and their normative constructs, assessing Indonesia and Thailand's regulatory frameworks, and analyzing the challenges and potential directions for future legal developments.

²⁰ Joanna Strycharz et al., "No to Cookies: Empowering Impact of Technical and Legal Knowledge on Rejecting Tracking Cookies," *Computers in Human Behavior* 120 (2021): 1-11, <https://doi.org/https://doi.org/10.1016/j.chb.2021.106750>.

²¹ Masitoh Indriani and Annida Aqiila Putri, "Persetujuan Dinamis Sebagai Sarana Optimalisasi Pelindungan Data Pribadi Dan Hak Atas Privasi," *Jurnal HAM* 14, no. 2 (August 2023): 105-22, <https://doi.org/10.30641/ham.2023.14.105-122>.

²² Chanchai Phonthanukitithaworn and Carmine Sellitto, "A Willingness to Disclose Personal Information for Monetary Reward: A Study of Fitness Tracker Users in Thailand," *SAGE Open* 12, no. 2 (2022): 1-15, <https://doi.org/10.1177/21582440221097399>.

III. Research Methods

This study employs the normative legal research method to base the analysis on the existing legal norms of the relevant legal frameworks.²³ Typical normative legal study, at least in its purest sense, involves the analysis of a particular legal issue through the lens of secondary data in the form of primary law sources, to allow a deep understanding of how a particular legal issue is seen according to the relevant legal norms.²⁴ To support the analysis of normative analysis on Indonesia and Thailand's relevant legal frameworks, this study also utilizes the comparative approach, to assess the relevant Indonesian and Thai framework for consumer data protection in the context of advanced data tracking. This approach is essential for the analysis as it enables the comparison between not only the existing legal framework from both countries, but also the gaps that are found within each of them. This is fundamentally based on the very purpose of comparative approach itself in the context of legal study, which is to find the similarities and differences, to ultimately obtain what is referred to as the common denominator of the legal issue within the legal topic at hand.²⁵ Secondary data used in this research are Law No. 27 of 2022 on Personal Data Protection, the 1945 Constitution, Personal Data Protection Act of Thailand, and the 2017 Constitution of Thailand, along with the Universal Declaration of Human Rights, which serves as the basic foundation for the human rights perspective.

IV. Result and Discussion

1. Boundaries of Data Tracking Technologies in the Digital Economy and their Normative Constructs

Digital transformation, at its core, cannot be separated from economic motivations.²⁶ While people and experts can argue about how digital transformation can improve communication, social activities, socio-cultural developments, and even entertainments,²⁷ profits remain one of the main drivers behind digital innovations and growth.²⁸ In the purely economics perspective, the supporting aspects of these developments naturally becomes the key focus of stakeholders of every market. Not only that, the tech industry as the core industry of the digital era²⁹ is also fixated on the aspects that can help propel the industry to higher heights. This is where data plays a crucial role as one of the key aspects that can help improve research and development (R&D) of the tech industry and many businesses that utilize digital technologies.³⁰

First, it is important to recognize the importance of data in shaping the development of digital technologies and the betterment of humanity. Data has long been a key aspect of scientific development, making it, at least what is considered by many people, an inevitable part of modern human civilization.³¹ Therefore, from the legal perspective, it is imperative to give enough room

²³ Hari Sutra Disemadi, "Lenses of Legal Research: A Descriptive Essay on Legal Research Methodologies," *Journal of Judicial Review* 24, no. 2 (2022): 289-304, <https://doi.org/10.37253/jjr.v24i2.7280>.

²⁴ David Tan, "Metode Penelitian Hukum: Mengupas Dan Mengulas Metodologi Dalam Menyelenggarakan Penelitian Hukum," *NUSANTARA: Jurnal Ilmu Pengetahuan Sosial* 8, no. 5 (2021): 2463-78, <https://jurnal.um-tapsel.ac.id/index.php/nusantara/article/view/5601>.

²⁵ Michael Bogdan, *Pengantar Perbandingan Sistem Hukum*, ed. Nurainun Mangunsong, trans. Derta Sri Widowatie, 2nd ed. (Bandung: Nusamedia, 2019).

²⁶ Tsotne Zhghenti and Lazare Kapanadze, "Sustainable Innovation in the Digital Age: Analyzing the Motivations of the Young Generation in Joining the Sharing Economy," *SocioEconomic Challenges* 8, no. 2 (July 2024): 1-11, [https://doi.org/10.61093/sec.8\(2\).1-11.2024](https://doi.org/10.61093/sec.8(2).1-11.2024).

²⁷ Sascha Kraus et al., "Digital Transformation: An Overview of the Current State of the Art of Research," *Sage Open* 11, no. 3 (July 2021): 1-15, <https://doi.org/10.1177/215824402111047576>.

²⁸ Titis Sri Wulan et al., "Digital Transformation as a Catalyst for SMEs Productivity and Profitability in the Digital Era," *Journal of Economic Education and Entrepreneurship Studies* 5, no. 4 (November 2024): 601-11, <https://doi.org/10.62794/je3s.v5i4.4543>.

²⁹ Jun Tu, "Green University: The Important Influencing Factor of Regional Development," *Advances in Social Science, Education and Humanities Research (ASSEHR)* 237 (2018): 204-9, <https://doi.org/10.2991/hsmet-18.2018.38>.

³⁰ Jingran Wang et al., "Overview of Data Quality: Examining the Dimensions, Antecedents, and Impacts of Data Quality," *Journal of the Knowledge Economy* 15, no. 1 (2024): 1159-78, <https://doi.org/10.1007/s13132-022-01096-6>.

³¹ André Dao, "Resisting the Inevitable: Human Rights and the Data Society," *London Review of International Law* 11, no. 2 (2023): 315-48, <https://doi.org/10.1093/lril/lrad012>.

for data collection and processing to ensure that developments of digital technologies and other relevant aspects of modern human life can continue and eventually bring many benefits for humanity overall. In the commercial context, data is also important for businesses to improve their product and services, even before the mass adaptation of digital technologies.³² With the utilization of digital technologies and the rise of digital economy, data plays an even more important and strategic role in ensuring seamless developments of businesses by providing wider consumer reach and unlocking many potentials for consumer personalization.

Consumer reach expansion is reliant on the quantity and quality of data acquired through various data collection methods,³³ as it helps identify potential consumers using a wide variety of data classifications. From sex and address, to occupation and spending habits, data can help businesses expand the reach of their products through offerings and advertising that are targeted to certain people according to these data. In the digital economy, this usage is even more prevalent as data tracking technologies can even help digital system providers key insights regarding a user's browsing habits, frequent clicks, interests, and even time spent on a particular webpage.³⁴ These relevant digital system providers would then offer their insights and understanding of their users' behavior patterns in the form of targeted advertising, for businesses who want to easily and seamlessly expand their reach without having to do in-depth market research.³⁵

The insights acquired from data tracking technologies are also utilized for consumer personalization.³⁶ Consumer personalization allows developers of electronic systems to provide relevant advertising and services that suit the browsing and usage patterns of their users.³⁷ Businesses can also directly take advantage of this digital capability, especially when they have their own websites to sell their products or services. Not only that, digital technologies can also help them manage exhaustive amount of data that they originally have, to then be processed digitally to support further analysis. Furthermore, businesses that have digitalized their operational practices can also provide their data to a third party to have their consumer's digital data analyzed using data tracking technologies. These data tracking utilizations typically involve data in the form of cookies and other relevant data, to provide extensive details about a consumer's digital behavior patterns.³⁸ In recent years, data tracking technologies have become even more advanced, expanding the capabilities through the utilization of artificial intelligence (AI), which speeds up the process of data tracking to give a more consistent tracking results.

Ultimately, these utilizations of data have created an ecosystem of data collection and processing, which have now become essential in the digital economy. This is not necessarily a problem as long as the practice of data collection and processing must be done in accordance to

³² Nadeem U. Shahid and Nasir J. Sheikh, "Impact of Big Data on Innovation, Competitive Advantage, Productivity, and Decision Making: Literature Review," *Open Journal of Business and Management* 09, no. 02 (2021): 586–617, <https://doi.org/10.4236/ojbm.2021.92032>.

³³ Muh Akbar M et al., "Development of Sustainable Business Models through Internal Partnerships Efforts to Expand Consumer Reach," *International Journal of Current Science Research and Review* 07, no. 03 (March 2024): 1904–9, <https://doi.org/10.47191/ijcsrr/V7-i3-52>.

³⁴ Abdul Qayoom et al., "Data-Driven Exploration of Web Browsing Habits: A Visual Analysis with BHVis," *The Asian Bulletin of Big Data Management* 3, no. 1 (December 2023): 125–34, <https://doi.org/10.62019/abbdm.v3i1.59>.

³⁵ Kirsten Martin and Katie Shilton, "Putting Mobile Application Privacy in Context: An Empirical Study of User Privacy Expectations for Mobile Devices," *Information Society* 32, no. 3 (2016): 200–216, <https://doi.org/10.1080/01972243.2016.1153012>.

³⁶ Katerina Volchek et al., "Co-Creating Personalised Experiences in the Context of the Personalisation-Privacy Paradox," in *Information and Communication Technologies in Tourism 2021*, ed. Wolfgang Wörndl, Chulmo Koo, and Jason L Stienmetz (Cham: Springer International Publishing, 2021), 95–108.

³⁷ Klaus M Miller and Bernd Skiera, "Economic Consequences of Online Tracking Restrictions: Evidence from Cookies," *International Journal of Research in Marketing* 41, no. 2 (2024): 241–64, <https://doi.org/https://doi.org/10.1016/j.ijresmar.2023.10.001>.

³⁸ Maosheng Yang et al., "Understanding the Impact Mechanism of User Behavior Pattern toward Real Estate APP Platforms in the Post-COVID Era: A Quantitative Analysis," *Sustainability*, 2023, <https://doi.org/10.3390/su15118926>.

key principles of privacy,³⁹ especially in the context of consumer data protection. These principles are key in setting up the boundaries in data collection and data processing, regardless of the purposes involved. However, due to the sheer volume of data that is collected and processed, the risks associated with data privacy and security might not be able to be fully accounted for. Empirical evidence supports this notion, as emerging risks of data privacy and security concerns are not necessarily met in Thailand, especially among SMEs, with an average score of around 6 out of 100 in a multi-criteria privacy policy scoring model consisting of 10 privacy principles and 31 privacy criteria developed by a study conducted by Chatsuwan et al. (2023).⁴⁰ Indonesia has also suffered from data-related problems, such as breach in the e-commerce sector involving 91 million users and the country itself being ranked third globally for highest data hacking rate.⁴¹

Transparency is a cornerstone of consumer data protection, particularly in the context of advanced tracking technologies such as cookies, pixels, and device fingerprinting.⁴² Digital system providers and businesses operating digitally must ensure that consumers are fully informed about what data is being collected, how it will be used, and who will have access to it. Consent must be explicit, freely given, and revocable at any time. This is especially important in advanced tracking technology utilizations, as they often use many forms of data that users are not aware of. This principle ensures that consumers maintain control over their personal information and are not unknowingly subjected to invasive tracking practices. A loophole that should not exist in this aspect is the utilization of bundled consent, which can be too overwhelmingly complex for the regular digital consumers to understand, essentially making it a manipulative and problematic advanced data collection practice.⁴³

Another critical boundary is the principle of data minimization. Businesses that operate digitally, including digital platforms themselves, should only collect data that is directly relevant and necessary for a specific purpose, avoiding excessive or unnecessary data collection.⁴⁴ Advanced tracking technologies should not gather sensitive personal information unless absolutely required and with explicit user consent. Additionally, the purpose limitation principle dictates that data collected for one purpose cannot be repurposed without notifying users and obtaining their consent again. Embedding these principles into the design of digital systems ensures compliance with privacy regulations while fostering consumer trust. This consistency of data usage strictly according to the consent agreement is fundamentally rooted in the core legal concept of *pacta sunt servanda*, where agreements between parties are considered as laws to those parties⁴⁵.

Most importantly, the enforcement of these boundaries must be met with efficient mechanisms, that would allow better enhanced protection of data privacy rights, particularly for consumers. This heightened focus on enforcement mechanism is important in the face of advanced data tracking technology, which might require sophisticated utilization relevant technology, supported by adequate normative structures. This mechanism would also need to facilitate immediate intervention to prevent further breaches of consumer privacy rights, which

³⁹ Sam Aiello, "Privacy Principles and Harms: Balancing Protection and Innovation," *Journal of Cybersecurity, Education, Research and Practice* 2024, no. 1 (2024): 1-9.

⁴⁰ Chatsuwan et al., "Personal Data Protection Compliance Assessment: A Privacy Policy Scoring Approach and Empirical Evidence from Thailand's SMEs."

⁴¹ Ari Wibowo, Widya Alawiyah, and Azriadi, "The Importance of Personal Data Protection in Indonesia's Economic Development," *Cogent Social Sciences* 10, no. 1 (December 31, 2024): 1-13, <https://doi.org/10.1080/23311886.2024.2306751>.

⁴² Tobias Dehling, Yuchen Zhang, and Ali Sunyaev, "Consumer Perceptions of Online Behavioral Advertising," in *Proceedings - 21st IEEE Conference on Business Informatics, CBI 2019*, vol. 1, 2019, 345-54, <https://doi.org/10.1109/CBI.2019.00046>.

⁴³ Leon Trakman, Robert Walters, and Bruno Zeller, "Digital Consent and Data Protection Law—Europe and Asia-Pacific Experience," *Information and Communications Technology Law* 29, no. 2 (2020): 218-49, <https://doi.org/10.1080/13600834.2020.1726021>.

⁴⁴ Md Abdul Malek, "Bigger Is Always Not Better; Less Is More, Sometimes: The Concept of Data Minimization in the Context of Big Data," *European Journal of Privacy Law and Technologies* 2021, no. 1 (2021): 212-23.

⁴⁵ Cemre Bedir, "Contract Law in the Age of Big Data," *European Review of Contract Law* 16, no. 3 (2020): 347-65, <https://doi.org/10.1515/ercl-2020-0020>.

would also require a certain level of expertise. This is where the role of Data Protection Officers (DPOs), who would significantly benefit from having an organizational support in the form of specific government body.

2. Assessment of Indonesia and Thailand's Regulations Regarding Data Tracking Technologies

Indonesia and Thailand have both tried to develop their own set of regulations to regulate data governance. This was mainly driven by the fact that digital technologies are getting increasingly reliant on data,⁴⁶ positioning data as a valuable asset that some would even refer to as “the new oil”.⁴⁷ Data is used across all aspects of research and development for every digital technology,⁴⁸ much like how utilization of data is present in all aspects of market research for all businesses who want to improve their products and services. In the context of consumer data protection, data is not only seen as something that needs to be protected in the general sense, but also a part of consumer's rights. In the human rights perspective, the protection of consumer data is even more important in the ever-so-digitalized world, specifically the rights to privacy, which is increasingly threatened by invasive advanced data tracking technologies.

To assess the relevant Indonesian and Thai frameworks for data protection and privacy, it is first important to provide the lens of normative exploration that would not only sharpen the analysis but also provide a clearer set of implications on the potential issues within those frameworks. For this matter, this study employs the theory of natural law, as it is the most suitable one for the perspective of human rights, which is a cornerstone of this study's perspective. The theory of natural law in this analysis is taken from the explanation made by Lon Fuller, who denies the separation of “is” and the “ought” in law, fusing the normative and factual element of law, contrasting the positivist theory of law.⁴⁹ It is based on the foundational understanding that any legal system is bound by universal moral values to fully realize its goal of ensuring the supremacy of law.⁵⁰

It is also imperative to recognize that consumer data protection has inherent conceptual differences and thus, also different legal implications, to the generalized understanding of data protection. Consumer data protection focuses on the protection of consumer's data, particularly in the realm of commerce, where e-commerce platforms and businesses who operate digitally are increasingly pushing the boundaries and risks of data privacy risks through their utilization of advanced data tracking technologies. Therefore, when viewed through the lens of human rights, this discourse has to also be in line with key principles of consumer protection, such as transparency and fairness.

First, it's important to look at the development of data tracking technologies to assess the urgency to analyze the normative adequacy of Indonesian and Thai data protection regulations in tackling them. Data tracking technologies were first introduced in 1996 with the emergence of third-party web trackers, which enabled systematic logging of user interactions and data flows across different websites.⁵¹ Fast forward, data tracking has continued to evolve using the combinations of newer technologies. Advanced data tracking technologies, are digital technologies that combine the use of technologies like artificial intelligence (AI), pixels, and

⁴⁶ Aneri Vasani et al., “Digital Data Forgetting: A Machine Learning Approach,” *International Journal for Research in Applied Science and Engineering Technology* 10, no. 4 (April 2022): 2645–48, <https://doi.org/10.22214/ijraset.2022.41743>.

⁴⁷ Christoph Stach, “Data Is the New Oil—Sort of: A View on Why This Comparison Is Misleading and Its Implications for Modern Data Administration,” *Future Internet* 15, no. 2 (2023): 1–49, <https://doi.org/10.3390/fi15020071>.

⁴⁸ Michael Blackburn et al., “Big Data and the Future of R&D Management,” *Research-Technology Management* 60, no. 5 (September 2017): 43–51, <https://doi.org/10.1080/08956308.2017.1348135>.

⁴⁹ Dennis Ejikeme Igwe and Godwin Udoh Udoh, “Law and Society: A Discourse on Lon Fuller's Principles of Law,” *Nnadiabube Journal of Philosophy* 7, no. 2 (May 18, 2024): 32–45, <https://acjol.org/index.php/NJP/article/view/4701>.

⁵⁰ Muklis Al'anam, “Moralitas Hukum Dalam Pemikiran Lon Fuller, H.L.A. Hart, Dan Hans Kelsen,” *Law Jurnal* 5, no. 2 (February 13, 2025): 146–57, <https://doi.org/10.46576/lj.v5i2.6015>.

⁵¹ Adam Lerner et al., “Internet Jones and the Raiders of the Lost Trackers: An Archaeological Study of Web Tracking from 1996 to 2016,” in *Proceedings of the 25th USENIX Security Symposium* (Austin: Usenix Association, 2016), 997–1013.

digital identifications. These technologies allow for a more specific and perhaps invasive tracking capabilities using data that are collected through various methods. Unlike the regular data analytics which utilizes Big Data and Internet of Things (*IoT*), advanced data tracking deploys machine learning algorithms to analyze cross-device behavioral patterns through pixel tracking and digital identifiers, creating persistent user profiles that evade traditional privacy frameworks.⁵²

Indonesia's main legal framework that governs data protection is Law No. 27 of 2022 on Personal Data Protection (PDP Law). This law is the results of years of precarious legislative efforts to improve digital governance, particularly in the specific focus of data. This law defines personal data protection through Article 1 number 2 as, "the overall effort to protect Personal Data in the course of processing of Personal Data in order to guarantee the constitutional rights of Personal Data subjects." In the PDP Law, data tracking normatively falls into "data processing", as governed in Article 16 paragraph (1), which includes "processing and analysis" as an example of data processing activity through letter b.

Consent is governed in Article 21, which details the responsibility of data collectors/processors in requiring an informed consent regarding data collection and processing. It is important to note that informed consent is a conceptually strict normative aspect within consumer data protection sphere, which this provision has normatively displayed. However, in the context of advanced data tracking, the normative aspects in Article 21 are not enough to ensure that data collectors and processors are giving enough information regarding how all the data is being collected and processed. Ultimately, article 21's informed consent framework has significant weaknesses in addressing advanced data tracking technologies because it fails to require disclosure of how multiple tracking mechanisms work in combination to create persistent cross-platform behavioral profiles that can bypass traditional privacy frameworks through real-time data triangulation and algorithmic analysis.

For Thailand, the main legal framework for data protection is Personal Data Protection Act (PDPA), which was enacted in 2019. This law governs various aspects of data protection, much like the PDP Law. The PDPA does not define data protection per se, rather establishes frameworks and mechanisms for protecting personal data through requirements for collection, use, and disclosure of personal data, as well as rights of data subjects and obligations of data controllers and processors. The most basic protection regarding consent by the PDPA is given through Section 19 which states that, "The Data Controller shall not collect, use, or disclose Personal Data, unless the data subject has given consent prior to or at the time of such collection, use, or disclosure, except the case where it is permitted to do so by the provisions of this Act or any other laws."

The same section, particularly in the fourth paragraph, also governs that "the entering into the contract, including any provisions of the service shall not be a condition to obtaining consent for the collection, use, or disclosure of Personal Data that is not necessary or not related to such contract entering, including the provisions of the service". This provision, combined with the basic one earlier, makes the PDPA superior in preventing consent bundling, as it requires a crystal clear, easily digestible, non-manipulative informed consent, which is not something that the Article 21 of the PDP Law provides. Most importantly, the provision from Section 19 of the PDPA is more suited to cover the complex nature of advanced data tracking, especially in the case of third-party data tracking involving different behavioral profiles in many digital platforms, which has been known to be quite invasive.⁵³ This puts the PDPA closer to the gold standard of privacy, the European Union's General Data Protection Regulation (GDPR),⁵⁴ which also governs the provision against consent bundling.⁵⁵

⁵² Sim, Heo, and Cho, "Combating Web Tracking: Analyzing Web Tracking Technologies for User Privacy."

⁵³ Timothy Libert, "Exposing the Hidden Web: An Analysis of Third-Party HTTP Requests on 1 Million Websites," *International Journal of Communication* 9, no. 1 (2015): 3544-61.

⁵⁴ Alessandro Mantelero, "The Future of Data Protection: Gold Standard vs. Global Standard," *Computer Law & Security Review* 40 (2021): 1-5, <https://doi.org/https://doi.org/10.1016/j.clsr.2020.105500>.

⁵⁵ Christine Utz et al., "(Un)Informed Consent: Studying GDPR Consent Notices in the Field," in *Proceedings of the ACM Conference on Computer and Communications Security*, 2019, 973-90, <https://doi.org/10.1145/3319535.3354212>.

Most importantly, it is also apparent that data classification remains the biggest weakness in both Indonesia's PDP Law and Thailand's PDPA, in the face advanced data tracking technologies. The lack of comprehensive data classification in this context provides a gaping loophole that can be abused by digital system providers and businesses who operate digitally. For example, in pixel tracking, pixels are not considered a part of data that are protected by both regulations. Thus, it can be collected however many and for whatever purposes, as there is no regulation that govern anything against any data collection and processing regarding this specific form of data. This essentially renders the rest of the provisions within the both PDP Law and PDPA ineffective, as they cannot be applied to the protection of pixels as data that are protected.

Both Indonesia and Thailand are also not equipped to facilitate consumer data protection in case of data breach. The PDP Law and the PDPA both require 72 hours of data breach notifications, which is far from the nature of advanced data tracking, where data collections and processing can all happen in short amount of time. The high-speed nature of the current digital landscape is perhaps the most prevalent in this phenomenon, particularly with the addition of AI and other digital capabilities. Speaking of AI, the PDP Law and PDPA also have no mention of algorithm transparency, which makes it extremely difficult to analyze data breach issues, as digital system providers and businesses that operate digitally are not obligated by law to disclose their algorithm's mechanism in data collection, processing, and most importantly, security. Despite seemingly technical in nature, these compliances are still not in line with the very purpose of data protection regime, which is to secure the privacy and the security of data, along with the interests of data subjects. These gaps show that the legal developments in Indonesia and Thailand have not yet met the core standard of natural theory, as in this case, the moral purpose of law in protecting privacy as a core human right cannot be fully facilitated, particularly in the face of advanced data tracking technologies.

From the human rights perspective, it is clear that Indonesia and Thailand are not sufficiently providing enough consumer data protection provisions in the face of threats to data privacy presented by advanced data tracking technologies. This is conceptually a significant shortcoming when looked through the constitutional lens of both countries. The natural law standpoint regarding this is also supported by the foundational legal norms found in both countries' constitution, along with core international acknowledgement of human rights. Indonesia's constitution, the 1945 Constitution, does not explicitly govern the right to privacy. However, Article 28G paragraph (1) of the 1945 Constitution governs the right to personal security, which encompasses protection from threats to privacy and freedom from interference in personal matters. Thailand governs the constitutional right to privacy in section 32 of the 2017 Thai Constitution, which states that, "*A person shall enjoy the rights of privacy, dignity, reputation and family.*" Furthermore, the normative issues identified also display the lack of care to a right that has been universally acknowledged, mainly through Universal Declaration of Human Rights (UDHR) Article 12, which states that, "*No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation.*" With the importance of implementing these foundational legal norms as moral compass for a legal system, there is an urgency to continuously develop the legal frameworks to fit the standard of today's technologies and their associated risks to privacy, which according to the natural law perspective, can support the supremacy of law to create order in society.

3. Challenges and Potentials in Future Legal Developments

As the global economy continues to evolve and adapts more digital technologies that are constantly being developed, legal systems around the world must find a way not only to consolidate their existing regulatory frameworks with emerging technologies, but also ensure that they can provide adequate protection for the interests of many people. This is exactly the main challenge that both Indonesia and Thailand are currently facing, as they are seeing an unprecedented level of digital technology adaptation, followed by immense economic growth. Legal development, from this perspective, becomes an inevitable reality if both countries do not

want to risk massive uncontrolled commercialization of consumers data, which will inevitably lead to privacy breaches and exploitation of personal information in their rapidly digitalizing economies.

Based on the weaknesses identified within Indonesian and Thai framework for consumer data protection, it is apparent that there is an urgent need for both countries to amend their respective frameworks in the face of serious privacy threats presented by advanced data tracking technologies. To tackle these weaknesses, this study proposes a model of legal development that can be used by both Indonesia and Thailand to enhance their consumer data protection regulations in the face of advanced data tracking technologies. Below is the table consisting the proposed model of legal development made specifically to tackle the identified issues within the PDP Law and PDPA.

Table 1: Proposed model of legal development to tackle privacy issues in data tracking technologies.

Normative Issue	Current Gap	Proposed Reform
Data Classification	No classification framework for ML-enabled pixel tracking, digital fingerprints, and cross-device behavioral data (Both Indonesia & Thailand)	Create comprehensive taxonomy for advanced tracking data types with specific protections for persistent identifiers
Algorithmic Transparency	No requirements for disclosure of tracking algorithms and data flows (Both Indonesia & Thailand)	Mandate transparency in ML-driven behavioral profiling mechanisms
Real-time Protection	72-hour breach notification inadequate for high-speed tracking systems (Both Indonesia & Thailand)	Implement immediate detection and response systems for tracking data breaches in digital platforms/systems that utilize advanced data tracking
Consent Framework	Lack of explicit prohibition against consent bundling (Indonesia only)	Mandate clear, unbundled consent mechanisms for tracking purposes

Source: Researcher Findings

This model specifically targets the weaknesses that have been identified previously, namely data classification, algorithmic transparency, and the lack of real-time protection. Overall, this model pushes for a more advanced understanding of the nature of advanced data tracking technologies, which both the Indonesian and Thai framework currently lack. This model also addresses the Indonesia-specific normative issue regarding consent, which is still behind Thailand. It is imperative to note that this model is not made to put extra burden on digital system providers and businesses who operate digitally, but rather create a framework for responsible data collection and processing, through systems that these key actors already have in place and running.

Aside from the proposed model of legal development above, both Indonesia and Thailand also need to take into serious account future challenges of consumer data protection. In the ever-so-digitalized commercial world, the use of quantum computing, which is currently being developed and supported with massive capitals, can present risks to data privacy like never seen before. Not only that, the increasing capability of AI, will also further complicate the issue of data management in the context of advanced tracking technologies. To at least make it easier for Indonesia and Thailand to adopt to these future challenges, closing the legal gaps with the current existing challenge becomes the utmost priority, to lessen the burden of future legislative goals.

V. Conclusion

The heart of the discourse of consumer data protection from the lens of human rights is ultimately privacy. Unfortunately, analysis of this study has found multiple weaknesses within the Indonesian and Thai framework for consumer data protection, underscoring the lack of protection to consumer privacy rights in the digital sphere. This study proposes a model of legal development that specifically addresses these weaknesses, namely the lack of advanced data classification and taxonomy, algorithmic transparency, and real-time protection. It is also important to note that Indonesia is behind Thailand regarding this discourse, as it has a normative structure that can be exploited for consent bundling, which the proposed model also addresses.

Ultimately, this discourse is a critical effort in ensuring that the right to privacy remains a human that is properly addressed and protected legally in Indonesian and Thai legal system, by ensuring the continuation of discuss in the academic realm. Moreover, the insights of this study serve can also serve as practical considerations for lawmakers in Indonesia and Thailand, who are tasked with the heavy responsibility of ensuring proper development of the digital space while also maintain the protection of key human rights, such as the right to privacy. Further research can explore more on the technical side of this discourse and hopefully develop a comprehensive data taxonomy for the data classification issue, which requires extensive technological expertise and about data tracking. This can be supported even further by future research, with the collection of empirical evidence regarding the concerns among consumers within the digital space, to strengthen the developed model as a solution to an the problem of privacy protection.

References

- Adwan, Ahmad Al, Husam Kokash, Raed Al Adwan, and Amira Khattak. "Data Analytics in Digital Marketing for Tracking the Effectiveness of Campaigns and Inform Strategy." *International Journal of Data and Network Science* 7, no. 2 (2023): 563-74. <https://doi.org/10.5267/j.ijdns.2023.3.015>.
- Aiello, Sam. "Privacy Principles and Harms: Balancing Protection and Innovation." *Journal of Cybersecurity, Education, Research and Practice* 2024, no. 1 (2024): 1-9.
- Akbar M, Muh, Muhammad Rakib, Andika Isma, and Dian Anugrah Sanusi. "Development of Sustainable Business Models through Internal Partnerships Efforts to Expand Consumer Reach." *International Journal of Current Science Research and Review* 07, no. 03 (March 2024): 1904-9. <https://doi.org/10.47191/ijcsrr/V7-i3-52>.
- Al-Zoubi, Waleed K. "Economic Development in the Digital Economy: A Bibliometric Review." *Economies* 12, no. 3 (2024): 1-28. <https://doi.org/10.3390/economies12030053>.
- Al'anam, Muklis. "Moralitas Hukum Dalam Pemikiran Lon Fuller, H.L.A. Hart, Dan Hans Kelsen." *Law Jurnal* 5, no. 2 (February 13, 2025): 146-57. <https://doi.org/10.46576/lj.v5i2.6015>.
- Bedir, Cemre. "Contract Law in the Age of Big Data." *European Review of Contract Law* 16, no. 3 (2020): 347-65. <https://doi.org/10.1515/ercl-2020-0020>.
- Bilal, Muhammad, Yunfeng Zhang, Shukai Cai, Umair Akram, and Alrence Halibas. "Artificial Intelligence Is the Magic Wand Making Customer-Centric a Reality! An Investigation into the Relationship between Consumer Purchase Intention and Consumer Engagement through Affective Attachment." *Journal of Retailing and Consumer Services* 77 (2024): 1-11. <https://doi.org/https://doi.org/10.1016/j.jretconser.2023.103674>.
- Blackburn, Michael, Jeffrey Alexander, J. David Legan, and Diego Klabjan. "Big Data and the Future of R&D Management." *Research-Technology Management* 60, no. 5 (September 2017): 43-51. <https://doi.org/10.1080/08956308.2017.1348135>.
- Bogdan, Michael. *Pengantar Perbandingan Sistem Hukum*. Edited by Nurainun Mangunsong. Translated by Derta Sri Widowatie. 2nd ed. Bandung: Nusamedia, 2019.
- Brkan, Maja. "The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way Through the Maze of the CJEU's Constitutional Reasoning." *German Law Journal* 20, no. 6 (2019): 864-83. <https://doi.org/DOI: 10.1017/glj.2019.66>.
- Chatsuwan, Panchapawn, Tanawat Phromma, Navaporn Surasvadi, and Suttipong Thajchayapong. "Personal Data Protection Compliance Assessment: A Privacy Policy Scoring Approach and Empirical Evidence from Thailand's SMEs." *Heliyon* 9, no. 10 (2023): 1-30. <https://doi.org/https://doi.org/10.1016/j.heliyon.2023.e20648>.

- Dao, André. "Resisting the Inevitable: Human Rights and the Data Society." *London Review of International Law* 11, no. 2 (2023): 315–48. <https://doi.org/10.1093/lril/lrad012>.
- Dehling, Tobias, Yuchen Zhang, and Ali Sunyaev. "Consumer Perceptions of Online Behavioral Advertising." In *Proceedings - 21st IEEE Conference on Business Informatics, CBI 2019*, 1:345–54, 2019. <https://doi.org/10.1109/CBI.2019.00046>.
- Delhi, Ariana, and Apriani Sijabat. "The Role of Technology Adoption in Scaling Startuppreneur Business Models in the Digital Economy." *Startuppreneur Business Digital (SABDA Journal)* 3, no. 2 (October 2024): 141–47. <https://doi.org/10.33050/sabda.v3i2.631>.
- Disemadi, Hari Sutra. "Lenses of Legal Research: A Descriptive Essay on Legal Research Methodologies." *Journal of Judicial Review* 24, no. 2 (2022): 289–304. <https://doi.org/10.37253/jjr.v24i2.7280>.
- Febriyani, Emiliya, Elza Syarief, and Triana Dewi Seroja. "Pemanfaatan Artificial Intelligence Dalam Deteksi Dan Pencegahan Tindak Pidana Pencucian Uang: Potensi Dan Tantangan Hukum?" *Jurnal Magister Hukum Udayana (Udayana Master Law Journal)* 13, no. 4 (2024): 877–98. <https://doi.org/10.24843/JMHU.2024.v13.i04.p10>.
- Gausman, Jewel, Niranjan Saggurti, Richard Adanu, Delia A.B. Bandoh, Mabel Berrueta, Suchandrima Chakraborty, Ernest Kenu, et al. "Validation of a Measure to Assess Decision-Making Autonomy in Family Planning Services in Three Low- and Middle-Income Countries: The Family Planning Autonomous Decision-Making Scale (FP-ADM)." *PLoS ONE* 18, no. 11 (2023): 1–17. <https://doi.org/10.1371/journal.pone.0293586>.
- Gerlich, Michael. "AI Tools in Society: Impacts on Cognitive Offloading and the Future of Critical Thinking." *Societies* 15, no. 1 (2025): 1–28. <https://doi.org/10.3390/soc15010006>.
- Igwe, Dennis Ejikeme, and Godwin Udoh Udoh. "Law and Society: A Discourse on Lon Fuller's Principles of Law." *Nnadiabube Journal of Philosophy* 7, no. 2 (May 18, 2024): 32–45. <https://acj.org/index.php/NJP/article/view/4701>.
- Indriani, Masitoh, and Annida Aqiila Putri. "Persetujuan Dinamis Sebagai Sarana Optimalisasi Pelindungan Data Pribadi Dan Hak Atas Privasi." *Jurnal HAM* 14, no. 2 (August 2023): 105–22. <https://doi.org/10.30641/ham.2023.14.105-122>.
- Kraus, Sascha, Paul Jones, Norbert Kailer, Alexandra Weinmann, Nuria Chaparro-Banegas, and Norat Roig-Tierno. "Digital Transformation: An Overview of the Current State of the Art of Research." *Sage Open* 11, no. 3 (July 2021): 1–15. <https://doi.org/10.1177/21582440211047576>.
- Lerner, Adam, Anna Kornfeld Simpson, Tadayoshi Kohno, and Franziska Roesner. "Internet Jones and the Raiders of the Lost Trackers: An Archaeological Study of Web Tracking from 1996 to 2016." In *Proceedings of the 25th USENIX Security Symposium*, 997–1013. Austin: Usenix Association, 2016.
- Libert, Timothy. "Exposing the Hidden Web: An Analysis of Third-Party HTTP Requests on 1 Million Websites." *International Journal of Communication* 9, no. 1 (2015): 3544–61.
- Lynskey, Orla. "Complete and Effective Data Protection." *Current Legal Problems* 76, no. 1 (November 2023): 297–344. <https://doi.org/10.1093/clp/cuad009>.
- Malek, Md Abdul. "Bigger Is Always Not Better; Less Is More, Sometimes: The Concept of Data Minimization in the Context of Big Data." *European Journal of Privacy Law and Technologies* 2021, no. 1 (2021): 212–23.
- Mantelero, Alessandro. "The Future of Consumer Data Protection in the E.U. Re-Thinking the 'Notice and Consent' Paradigm in the New Era of Predictive Analytics." *Computer Law & Security Review* 30, no. 6 (2014): 643–60. <https://doi.org/https://doi.org/10.1016/j.clsr.2014.09.004>.

- — —. “The Future of Data Protection: Gold Standard vs. Global Standard.” *Computer Law & Security Review* 40 (2021): 1-5. <https://doi.org/https://doi.org/10.1016/j.clsr.2020.105500>.
- Martin, Kirsten, and Katie Shilton. “Putting Mobile Application Privacy in Context: An Empirical Study of User Privacy Expectations for Mobile Devices.” *Information Society* 32, no. 3 (2016): 200-216. <https://doi.org/10.1080/01972243.2016.1153012>.
- Miller, Klaus M, and Bernd Skiera. “Economic Consequences of Online Tracking Restrictions: Evidence from Cookies.” *International Journal of Research in Marketing* 41, no. 2 (2024): 241-64. <https://doi.org/https://doi.org/10.1016/j.ijresmar.2023.10.001>.
- Phonthanukitithaworn, Chanchai, and Carmine Sellitto. “A Willingness to Disclose Personal Information for Monetary Reward: A Study of Fitness Tracker Users in Thailand.” *SAGE Open* 12, no. 2 (2022): 1-15. <https://doi.org/10.1177/21582440221097399>.
- Qayoom, Abdul, Shafiq Ur Rehman, Muhammad Waqas, Muhammad Aoun, Umair Saeed, Wu Yadong, and Wang Song. “Data-Driven Exploration of Web Browsing Habits: A Visual Analysis with BHVis.” *The Asian Bulletin of Big Data Management* 3, no. 1 (December 2023): 125-34. <https://doi.org/10.62019/abbdm.v3i1.59>.
- Riegger, Anne-Sophie, Jan F Klein, Katrin Merfeld, and Sven Henkel. “Technology-Enabled Personalization in Retail Stores: Understanding Drivers and Barriers.” *Journal of Business Research* 123 (2021): 140-55. <https://doi.org/https://doi.org/10.1016/j.jbusres.2020.09.039>.
- Rizal, Muhammad, and Erika Vivin Setyoningsih. “Perlindungan Konsumen Dalam Pemanfaatan Big Data Oleh Pelaku Bisnis Di Indonesia: Tinjauan Terhadap Regulasi Dan Implementasi Praktik Bisnis.” *Jurnal Penegakan Hukum Dan Keadilan* 4, no. 1 (2023): 75-85.
- Satwiko, Brahmantyo Suryo. “Privacy and Data Protection: Indonesian Legal Framework.” *Corporate and Trade Law Review* 1, no. 2 (2021): 98-118. <https://doi.org/10.21632/ctrl.1.2.98-118>.
- Setiartiti, Lilies, and Fitri Rahmadani. “Determinant of Economic Growth in ASEAN Countries (Indonesia, Thailand, Malaysia, Singapura, Philipines) 2010-2019.” *Journal of Economics Research and Social Sciences* 7, no. 2 (2023): 253-64. <https://doi.org/10.18196/jerss.v7i2.19551>.
- Shahid, Nadeem U., and Nasir J. Sheikh. “Impact of Big Data on Innovation, Competitive Advantage, Productivity, and Decision Making: Literature Review.” *Open Journal of Business and Management* 09, no. 02 (2021): 586-617. <https://doi.org/10.4236/ojbm.2021.92032>.
- Sim, Kyungmin, Honyeong Heo, and Haehyun Cho. “Combating Web Tracking: Analyzing Web Tracking Technologies for User Privacy.” *Future Internet*, 2024. <https://doi.org/10.3390/fi16100363>.
- Stach, Christoph. “Data Is the New Oil-Sort of: A View on Why This Comparison Is Misleading and Its Implications for Modern Data Administration.” *Future Internet* 15, no. 2 (2023): 1-49. <https://doi.org/10.3390/fi15020071>.
- Strycharz, Joanna, Edith Smit, Natali Helberger, and Guda van Noort. “No to Cookies: Empowering Impact of Technical and Legal Knowledge on Rejecting Tracking Cookies.” *Computers in Human Behavior* 120 (2021): 1-11. <https://doi.org/https://doi.org/10.1016/j.chb.2021.106750>.
- Sudirman, Lu, Rufinus Hotmaulana Hutaauruk, Hari Sutra Disemadi, and Agustianto Agustianto. “BEYOND LIKES AND FOLLOWS: Navigating Consumer Trust and IPR-Related Risks in Influencer Marketing.” *Jurisdictie: Jurnal Hukum Dan Syariah* 15, no. 2 (January 2025): 245-73. <https://doi.org/10.18860/j.v15i2.28054>.
- Suntsova, Olesia. “Digital Transformation of the Global Economy: Challenges and Opportunities.” *Financial and Credit Systems: Prospects for Development* 3, no. 14 (September

- 2024): 10–87. <https://doi.org/10.26565/2786-4995-2024-3-08>.
- Tan, David. “Metode Penelitian Hukum: Mengupas Dan Mengulas Metodologi Dalam Menyelenggarakan Penelitian Hukum.” *NUSANTARA: Jurnal Ilmu Pengetahuan Sosial* 8, no. 5 (2021): 2463–78. <https://jurnal.um-tapsel.ac.id/index.php/nusantara/article/view/5601>.
- Tolegenov, Bakyt, Kevin Rafif, Muhammad Rafi, Rafidah Herawati, Asaduddin Abdullah, and Linda Karlina Sari. “Digital Transparency and Consumer Awareness: Digital Platforms for Educating Consumers about Product Origins and Sustainability.” *AL-MUZARA’AH* 12, no. 2 (December 2024): 277–87. <https://doi.org/10.29244/jam.12.2.277-287>.
- Trakman, Leon, Robert Walters, and Bruno Zeller. “Digital Consent and Data Protection Law—Europe and Asia-Pacific Experience.” *Information and Communications Technology Law* 29, no. 2 (2020): 218–49. <https://doi.org/10.1080/13600834.2020.1726021>.
- Tu, Jun. “Green University: The Important Influencing Factor of Regional Development.” *Advances in Social Science, Education and Humanities Research (ASSEHR)* 237 (2018): 204–9. <https://doi.org/10.2991/hsmet-18.2018.38>.
- Utz, Christine, Martin Degeling, Sascha Fahl, Florian Schaub, and Thorsten Holz. “(Un)Informed Consent: Studying GDPR Consent Notices in the Field.” In *Proceedings of the ACM Conference on Computer and Communications Security*, 973–90, 2019. <https://doi.org/10.1145/3319535.3354212>.
- Vasani, Aneri, Sahana Shettigar, Snehlata Rana, and Prof. Shirish K Sabnis. “Digital Data Forgetting: A Machine Learning Approach.” *International Journal for Research in Applied Science and Engineering Technology* 10, no. 4 (April 2022): 2645–48. <https://doi.org/10.22214/ijraset.2022.41743>.
- Volchek, Katerina, Joanne Yu, Barbara Neuhofer, Roman Egger, and Mattia Rainoldi. “Co-Creating Personalised Experiences in the Context of the Personalisation-Privacy Paradox.” In *Information and Communication Technologies in Tourism 2021*, edited by Wolfgang Wörndl, Chulmo Koo, and Jason L Stienmetz, 95–108. Cham: Springer International Publishing, 2021.
- Wang, Jingran, Yi Liu, Peigong Li, Zhenxing Lin, Stavros Sindakis, and Sakshi Aggarwal. “Overview of Data Quality: Examining the Dimensions, Antecedents, and Impacts of Data Quality.” *Journal of the Knowledge Economy* 15, no. 1 (2024): 1159–78. <https://doi.org/10.1007/s13132-022-01096-6>.
- Whitney, Cedric Deslandes, and Justin Norman. “Real Risks of Fake Data: Synthetic Data, Diversity-Washing and Consent Circumvention.” In *The 2024 ACM Conference on Fairness, Accountability, and Transparency*, 1733–44. New York, NY, USA: ACM, 2024. <https://doi.org/10.1145/3630106.3659002>.
- Wibowo, Ari, Widya Alawiyah, and Azriadi. “The Importance of Personal Data Protection in Indonesia’s Economic Development.” *Cogent Social Sciences* 10, no. 1 (December 31, 2024): 1–13. <https://doi.org/10.1080/23311886.2024.2306751>.
- Wulan, Titis Sri, Reni Reni, Rezty Arizta Putri, and Dewi Agustina Solihin. “Digital Transformation as a Catalyst for SMEs Productivity and Profitability in the Digital Era.” *Journal of Economic Education and Entrepreneurship Studies* 5, no. 4 (November 2024): 601–11. <https://doi.org/10.62794/je3s.v5i4.4543>.
- Xu, Tao, Hanning Shi, Yongjiang Shi, and Jianxin You. “From Data to Data Asset: Conceptual Evolution and Strategic Imperatives in the Digital Economy Era.” *Asia Pacific Journal of Innovation and Entrepreneurship* 18, no. 1 (January 2024): 2–20. <https://doi.org/10.1108/APJIE-10-2023-0195>.
- Yang, Maosheng, Ping Li, Honghong Zhou, Zeyu Li, and Lei Feng. “Understanding the Impact

Mechanism of User Behavior Pattern toward Real Estate APP Platforms in the Post-COVID Era: A Quantitative Analysis." *Sustainability*, 2023. <https://doi.org/10.3390/su15118926>.

Zhghenti, Tsothe, and Lazare Kapanadze. "Sustainable Innovation in the Digital Age: Analyzing the Motivations of the Young Generation in Joining the Sharing Economy." *SocioEconomic Challenges* 8, no. 2 (July 2024): 1-11. [https://doi.org/10.61093/sec.8\(2\).1-11.2024](https://doi.org/10.61093/sec.8(2).1-11.2024).