

RESEARCH ARTICLE

Data and statecraft: why and how states localize data

Sanghyun Han 

Sam Nunn School of International Affairs, Georgia Institute of Technology, Atlanta, USA
Email: shhan@gatech.edu

Abstract

This paper explores the motives and mechanisms behind data localization implemented by states to protect data, which is essential to emerging technologies such as Artificial Intelligence. Despite the significant negative aspects of data localization for states, the practice has become increasingly prevalent, leading to the unexplored question of why states choose to implement it. This suggests that data localization is a form of economic means derived from digital technologies and employed by states to serve political objectives. Focusing on the data in platforms, the theoretical mechanism of data localization is captured in light of two factors: network perception and security externality. Network perception pertains to a state's perception of the positive network effect generated by platforms, while security externality refers to a state's consideration of the security implications in relation to the economic benefits derived from the positive network effect, serving the national interest in domestic and/or international contexts. To substantiate these theoretical propositions, the paper employs a comparative case study approach where Vietnam, Singapore, and Indonesia have been chosen as empirical cases based on the selection strategy. The paper bridges the concept of economic statecraft with digital technologies, fosters interdisciplinary discussions, and offers policy implications.

Keywords: data localization; digital regulation; economic statecraft; externality; network effect

Introduction

The exponential growth of internet users and their activities on platforms like Facebook, Instagram, and Amazon has resulted in vast amounts of user data being collected. In a single minute, approximately 4.5 billion internet users generate a staggering number of interactions, including 41 million WhatsApp messages, 13 million video or voice calls, and the upload of 147,000 pictures on Facebook.¹ These platforms utilize this data to offer personalized and profitable services to their users. However, within the context of geopolitical and technological competition, data takes on a completely different significance. The current international landscape is witnessing the rise of technonationalism, wherein states strive to lead and dominate in emerging technology sectors.² In particular, data is viewed as a strategic asset by many states, capable of providing a competitive edge in the field of artificial intelligence (AI).³ The debate revolves around whether a large quantity of data or a highly refined and precise dataset is more instrumental in the development of AI as a training set. While a large volume of data enables AI systems to quickly identify patterns and derive insights,⁴ high-quality data, characterized by accuracy and relevance, is essential for AI to make decisions that complement human judgment.⁵

Irrespective of this debate, it is indisputable that well-trained AI models, powered by data, have far-reaching implications for both domestic and international arenas, spanning civil and military

¹Ali (2020).

²Ding (2022).

³Ding and Dafoe (2021).

⁴O'Leary (2013).

⁵Goldfarb and Lindsay (2021).

applications. The influence of AI, driven by data, extends to national strategies, shaping human nature and influencing perceptions of the international structure.⁶ Its impact transcends boundaries and permeates various aspects of society, making it a critical consideration for policymakers and researchers alike. In this regard, it is understandable that states seek to safeguard their data from exploitation or unauthorized extraction by external actors. Notably, China has implemented some of the most stringent regulations on data, a measure that has contributed to its economic growth and technological advancement.⁷ Data localization, which requires businesses to establish new data centers within a country's borders, not only strengthens national data security but also generates economic benefits at both the national and local levels. The construction of data storage facilities contributes to the overall economy and has positive spillover effects on local communities.⁸ Consequently, data localization serves as a multifaceted strategy that addresses security concerns while simultaneously fostering economic development.

Though China's approach to data localization is unique, driven by its vast population and long-standing pursuit of the party's objectives.⁹ Drawbacks of data localization often outweigh the benefits. One significant concern is the negative impact on economic development. Empirical research demonstrates that data localization can hinder national economies, leading to declines in gross domestic product, investments, and trade.¹⁰ This approach has been criticized for impeding economic growth and innovation by restricting the free flow of data across borders.¹¹ 82 percent of large firms and 52 percent of small and medium-sized firms, based on the survey in the digital communication sector, considers data localization as a constraint.¹² Moreover, data localization imposes unexpected burdens on businesses. The costs associated with building new data centers or transitioning to local data storage can pose significant barriers, particularly for entities seeking to enter new markets.¹³ In situations where local or international cloud service providers are limited, platforms may be compelled to establish their own data centers or rely on less qualified local providers with limited digital infrastructure. Another concern is the potential compromise of data security. By mandating data storage within national borders, without duplication outside, the recovery of data in the event of a cyber attack or natural disaster becomes challenging.¹⁴ Lastly, data localization does not guarantee complete isolation from external access, as the nature of data transcends physical boundaries.¹⁵

The adoption of data localization measures has increased significantly in recent years, with the number of countries implementing such policies more than doubling since 2017.¹⁶ In fact, approximately 80 percent of nations now have data protection legislation or drafts in place.¹⁷ This raises an intriguing question: why do states choose to localize data for all the negative impacts it can have on their interests? To address this question and provide a coherent and theoretical explanation, this paper applies the concept of economic statecraft.¹⁸ Data localization is seen as an economic means derived from digital technology that serves political objectives. Given the broad applicability of data and its role in driving economic development and innovation, states view data localization not merely as a remedial measure but as a form of economic statecraft. The emergence of the platform economy further accentuates this question by challenging the perceived locus of value and authority between platforms and states.¹⁹ By perceiving data as a driver of economic growth, states impose barriers that restrict the

⁶Kissinger, Schmidt, and Huttenlocher (2021); Ayoub and Payne (2016).

⁷McKnight, M. Kenney, and Breznitz (2023).

⁸Pham (2017); VanLear et al. (2020); Levine (2018).

⁹Creemers (2022).

¹⁰Bauer et al. (2014); Cory, Dascoli, and Clay (December 12, 2022).

¹¹OECD (December 11, 2011); US Trade Representative (March 2017).

¹²US International Trade Commission (2014), 77–108.

¹³Chander and Lê (2015), 721–730.

¹⁴Swire and Kennedy-Mayo (2022), 13–29; Ryan, Falvey, and Merchant (2013), 57–58.

¹⁵Reisman (May 22, 2017).

¹⁶Cory and Dascoli (July 19, 2021).

¹⁷Parekh et al. (June 20, 2022).

¹⁸Baldwin (2020); Norris (2016), 13–15.

¹⁹M. Kenney and Zysman (2016).

flow of data, thereby controlling the economic benefits it can generate.²⁰ Mandating the localization of data storage is a sophisticated and highly articulated approach to regulating data, as it underscores a state's sovereign power. Consequently, data localization offers a unique perspective on data as an economic instrument with implications for security.

Data localization encompasses various definitions and degrees of restrictions imposed by states on data.²¹ For the purpose of this paper, data localization is defined as a policy implemented by a state that requires entities to store data within its sovereign territory. This definition emphasizes the role of the state as the primary actor responsible for enforcing such requirements on private entities. An example of this policy is when foreign entities are compelled to establish local data centers in the region.²² The term "platform" in this context refers to an entity that acts as an intermediary, connecting consumers and services in accordance with the definition of a transaction platform.²³ The data under consideration in this paper is the data generated by users within these platforms, excluding data with direct military applications.

This paper aims to examine the motivation and mechanism underlying data localization, with a particular focus on its connection to economic statecraft. The subsequent section investigates the relationship between states and three key data-relevant categories: individual referents, platforms, and structural characteristics. Moving forward, the paper presents a theoretical mechanism that emphasizes the need for a comprehensive and heuristic understanding rather than a one-sided approach. This mechanism establishes the significance of both network perception and security externality as essential factors in data localization. Network perception pertains to a state's perception of the positive network effect generated by platforms, while security externality refers to a state's consideration of the security implications in relation to the economic benefits derived from the positive network effect, serving the national interest in domestic and/or international contexts. To substantiate these theoretical propositions, the paper employs a comparative case study approach, utilizing process-tracing methodology and primary sources. Vietnam, Singapore, and Indonesia are selected as empirical cases, and the findings from the case study support the theoretical mechanism. In conclusion, this research bridges the concept of economic statecraft with digital technologies, fosters interdisciplinary discussions, and offers practical implications for policymakers.

Motives: why states localize data

States have varying motivations for implementing data localization policies, which can be categorized based on their interactions with three key actors: individual referents, platforms, and the structural characteristics of data itself.²⁴ The first category focuses on a state's responsibility to safeguard individuals' rights and privacy from potential encroachments by platforms. The second category highlights data localization as a tool for states to impose economic burdens on foreign platforms and nurture the growth of domestic platforms. The third category, highlighting the structural standpoint, examines the inherent constraints of data at the national level through intuitive thought experiments despite some caveats. It is important to note that these categories are not mutually exclusive but rather represent distinct driving forces behind the adoption of data localization policies.

The first motivation behind states implementing data localization measures is the protection and security of individuals' digital rights. Despite individuals having the ultimate decision-making power over providing their data to platforms or third parties, these rights are often violated in practice.

²⁰Meltzer (2020).

²¹González, Casalini, and Porras (2022); Basu, Hickok, and Chawla (March 19, 2019).

²²Ferracane (2017), 2–4.

²³(Cusumano, Gawer, and Yoffie 2019, 18–21). On the other hand, an innovation platform facilitates the interaction between users and producers of a system, such as the Google Android platform, which bridges users and designers of complementary systems. Hybrid platforms encompass features of both transaction and innovation platforms, and many major tech companies, including Amazon, Google, Facebook, and Tencent, fall into this category.

²⁴Obendiek (2022).

Platforms engage in excessive surveillance of users in order to gather as much data as possible.²⁵ This issue is exemplified by the Cambridge Analytica scandal, where improperly obtained data was used to create voter profiles for the 2016 US presidential election.²⁶ Such incidents have strengthened the public's demand for the protection of their data rights. Data localization serves to reinforce a state's belief that it can provide more explicit protection for these rights. It also contributes to the enhancement of rights protection by imposing specific obligations on platforms.²⁷ Since the regulations implemented by a state are influenced by its perception of the relationship between users and platforms, the "Rights of the data subject" outlined in the European Union's General Data Protection Regulation (GDPR) facilitates users' access to platform data applications and establish punitive measures for non-compliance.²⁸

Data localization serves as a means to address the dominance of a few US platforms and incentives the development of domestic platforms and capabilities. The nature of platform businesses makes them susceptible to a winner-takes-all or oligopolistic market structure. The larger the user base of a platform, the more data it accumulates, enabling it to provide better-tailored services based on the collected data.²⁹ This network effect creates a virtuous cycle that allows dominant platforms to maintain a significant market share. The widespread international presence of these dominant US platforms can raise concerns about consumer welfare in foreign countries, as their options become limited. Consequently, government intervention becomes necessary to protect consumer interests. The focus on enforcing antitrust laws in the United States and the ongoing legal battles between the US federal government and platform companies highlight the need for comprehensive socio-economic regulations.³⁰ Thus, data localization can be seen as a measure that enables states to address the skewed market dynamics and promote a more balanced ecosystem.

In addition, data localization measures can lead to discrimination between domestic and foreign platforms, providing advantages or protection to domestic platforms. This aspect of data localization aligns with the discussions on strategic trade policies in the 1970s, which aimed to protect domestic industries from external markets while stimulating the domestic market.³¹ Through simulations, it has been observed that data localization encourages local users to prefer domestic platforms by creating barriers for foreign platforms.³² Moreover, data localization can enhance the competitiveness of domestic platforms by familiarizing them with data regulations in other states and enabling them to adapt more easily. The economic burden of data localization on foreign entities, particularly those that need to comply by establishing local data centers or contracting with local storage providers, can significantly increase data hosting expenses by 30 to 60 percent.³³ However, the extent of this burden varies depending on factors such as the existing business infrastructure and the market size of the respective states. It is important to distinguish between mandatory data localization requirements imposed by regulatory authorities and voluntary market-driven decisions. Platforms are not necessarily required to store all local data within local storage facilities; instead, they often operate regional data centers to cover regional demands rather than catering solely to a single local market. Considering data storage facilities as critical infrastructure entails taking into account various factors.³⁴ The burgeoning demand for data localization by states within the same or neighboring regions can disrupt platforms' existing portfolios and business plans, imposing significant economic burdens.

The final perspective on data localization emphasizes the structural constraints imposed by the characteristics of data itself. Data is considered a quasi-public good, possessing a non-rivalrous nature

²⁵Bernal (2016); Beduschi (2019); Lau (2023).

²⁶Confessore (2018).

²⁷Bygrave (1998).

²⁸Mazurek and Ma lagoocka (2019); Intersoft Consulting (2020).

²⁹Anderson and Moore (2006).

³⁰Cioffi, M. F. Kenney, and Zysman (2022); Fukuyama, Richman, and Goel (2021); Na and Ma (2021); Bonatti et al. (2021).

³¹Abaraham Newman (2008), 10; Brander (1988); Tyson and Zysman (1983).

³²Potluri, Sridhar, and Rao (2020).

³³O'Connor (2015).

³⁴Guliani and Swift (2019).

with partial excludability, meaning that it can be perpetuated but it is challenging to distinguish between non-paying and paying users and deny access to the service.³⁵ This structural constraint of data underscores the regulatory power of domestic policies rather than the establishment of international data governance agreements, hindering the creation of a comprehensive global framework.³⁶ Given the nature of data, effective mechanisms for regulating its access and application need to be established at the national level. Although the interplay and strategies between states are complex and influenced by various factors such as the bilateral relationship, the number of players, economic and market power, repetition of rounds, and information sharing possibilities, simple thought experiments using scenarios can provide an intuitive understanding of data localization as a structural restraint.

The structural constraints inherent in data significantly influence the way states perceive and subsequently decide on whether to engage in cooperation or exploitation in the context of data localization. The perception between states, including the level of trust they have in each other, introduces a different dynamic.³⁷ Let us consider a scenario in which countries have commensurate sizes of internet-relevant indicators and are faced with a decision between enabling the free flow of data or implementing data localization. If the two countries engage in a single-game decision-making process, data localization emerges as the optimal choice for both countries. This can be illustrated using a prisoner's dilemma-like game. Exploiting others' data without exchanging one's own data yields the highest payoff. If one country decides to localize data while the other opts for free flow, the regulating country can exploit data generated by both countries. In a game played between trusted partners who view each other as reliable, however, pursuing the free flow of data leads to the highest payoff. Nevertheless, even if both countries choose data localization, it is likely to result in compatible data policies between the partners by increasing the similarity of data regulations. As the legal institutions become more aligned, facilitating information sharing between the two countries,³⁸ data localization within a cooperative game can strike a balance between the interests of the two states. Ultimately, a state's decision is intricately linked to its perception of the actions taken by another state, as illustrated in both hypothetical scenarios.

Localization mechanism

The multifaceted nature of data localization is reflected in the various motives associated with individuals, platforms, and structural constraints, highlighting it as a strategic choice made by states to pursue specific goals. However, it is important to avoid a narrow perspective that solely focuses on a single driver or discrete understanding, as it fails to fully explain the increasing trend of states adopting data localization measures and the underlying motivations behind their strategic decisions. As demonstrated in the previous section, no single motivation—referents, platforms, and structure derived from data—explains the entire calculation of data localization. This is because states engage in a calculated assessment and employ their own criteria when considering data localization. This is substantiated by the recent US withdrawal of the e-commerce rule proposal to the World Trade Organization, which aimed to “provide enough policy space for those debates.”³⁹ To capture this strategic dimension, which can be viewed as a form of economic statecraft derived from digital technology, a theoretical mechanism is proposed that incorporates the concepts of network perception and security externality in a heuristic way. By treating network perception and security externality as independent variables, the mechanism highlights their role as driving forces behind data localization, the dependent variable.

³⁵L. Liu (2021).

³⁶Chaisse (2023), 88–89.

³⁷Axelrod and R. O. Keohane (1985), 237–238.

³⁸Efrat and Abraham Newman (2018).

³⁹Lawder (October 25, 2023).

Network perception

In the realm of platform businesses, the significance of the data-driven network effect cannot be overstated. The network effect, defined as the impact of the number of agents taking equivalent actions on the net value of an action, holds particular relevance in this context.⁴⁰ When more users join a specific telecommunication vendor, for example, the vendor is compelled to enhance its service and coverage to meet the growing user demands. This improved quality of service then attracts additional users to join the vendor, creating a positive network effect. Conversely, if a network service vendor experiences an overwhelming influx of users, it can lead to a decline in the quality and speed of the network, prompting users to switch to alternative vendors. These scenarios, referred to as positive and negative network effects respectively, demonstrate the significant influence of network structure and performance on network value, in addition to user numbers.⁴¹ In platform businesses driven by data, the value of a platform network is directly linked to the data network effect which is positive network effect. This effect manifests as the platform's ability to provide personalized and tailored services based on the data it collects from users, thereby increasing its attractiveness and drawing in more users.⁴² Consequently, users often find it challenging to refrain from using these services once they have become accustomed to them.

The decision to implement data localization is influenced by a state's ability to harness and leverage the gains and benefits derived from the positive network effect. Platforms, with their control over user data and the ability to extract value from it, play a pivotal role in shaping the regulatory and political landscape of a nation.⁴³ This skewed relationship between states and platforms allows states to assess whether the network effect generated by platforms aligns with national interests and whether they can effectively utilize the resulting benefits. This relationship serves as an independent variable in driving data localization.

Network perception in this vein refers to a state's perception of the positive network effect generated within and/or by platforms. This network perception can be classified as either positive or negative. Positive network perception occurs when a state views the network effect as an opportunity or a contribution to its national interests. In other words, when a state can exploit and benefit from the network effect generated by local and/or foreign platforms, it is considered advantageous, particularly from an economic standpoint. Conversely, negative network externality arises when a state perceives the positive network effect as a form of dependence or vulnerability, unable to effectively utilize the value generated by it. If platforms that align with a state's objectives benefit from this network effect, it engenders a positive perception because these benefits ultimately contribute to the state's interests. However, if platforms are difficult to malleable, the state's perception becomes negative.

The presence of negative network perception reinforces the implementation of data localization, especially in the context of dominant foreign platforms in the market. The lopsided relationship between states and platforms contributes to a sense of vulnerability as foreign platforms increase domestic users' dependence on them. The winner-takes-all nature of the platform market and the notion of vulnerability⁴⁴ highlight the susceptibility of states to the influence of dominant foreign platforms. Once these platforms solidify their dominant position, both users and states incur costs or face limitations in trying to disengage from their services. The extraterritorial nature of dominant foreign platforms further limits the impact of state policies on societal influence. In response, data localization emerges as a strategic solution to alleviate negative perceptions and enable states to internalize the economic benefits and advantages derived from data localization. By doing so, states can impede foreign platforms and enhance their capacity for internalization, safeguarding their domestic capabilities and preventing foreign competitors from exploiting domestic assets.⁴⁵

⁴⁰Liebowitz and Margolis (1994), 135.

⁴¹Afuah (2013).

⁴²Bamberger and Lobel (2017), 1062–1070; Gregory et al. (2021).

⁴³Martens (2021), 9–20; Thelen (2018).

⁴⁴Hirschman (1980), 13–33; R. Keohane and Nye (2012), 3–19.

⁴⁵Buzan (2008), 197–213; Richardson (1990); Crawford (1993), 46–83.

Security externality

Platform business using data encompasses not only economic considerations but also security implications. One such implication arises when a government seeks or presumably possesses unrestricted access to the data accumulated by influential platforms. In an anarchic international system characterized by uncertainty, states may anticipate indefinite access to data and its potential military applications by potential adversaries. The concept of an informational-industrial complex, which highlights the possible collaboration between platform businesses and governments, further emphasizes the security dimension of data.⁴⁶ Within the context of the relationship between a host country and foreign platforms, states contemplate the worst-case scenario that foreign platforms might share the collected data with adversarial actors, given the dual-use nature of data.⁴⁷

Furthermore, the increasing power wielded by platforms amplifies the security concerns of states. Data, being an inexhaustible resource that fuels innovation in both commercial and military realms, holds immense value.⁴⁸ Platforms, by aggregating vast amounts of data, simulate a domestic legal and regulatory capacity that is typically the purview of states. This grants them significant influence over other sectors and allows them to exert regulatory power in the absence of state authority.⁴⁹ Additionally, the era of “surveillance capitalism” epitomizes the transfer of influential power to platforms, as they amass and store extensive data for their lucrative purposes.⁵⁰ Platforms, due to their significant power and influence, have a direct and complex relationship with various aspects of national security, encompassing both narrow and broad interpretations of the concept.⁵¹ This convergence of data-driven power and platform dominance further underscores the security implications for states.

The security implications associated with data localization serve as another significant driver for its adoption. These security considerations stem from the interplay between economic interactions and national security interests, particularly in relation to dual-use technologies and trade. Security externality, as a byproduct of economic gains from the positive network effect, manifests in two forms: internal and external. Both types can be classified as either positive or negative. Internal security externality pertains to the security ramifications of economic interactions within a nation’s domestic affairs and political landscape. The introduction of platforms can have a profound impact on a country’s internal dynamics. Domestic platforms, for instance, can empower domestic audiences, leading to outcomes that can be either positive or negative. This situation can present opportunities for certain states, as it reinforces democratic values and principles. However, it can also pose challenges for others by amplifying public voices that may be viewed as detrimental to national interests.⁵² External security externality, on the other hand, relates to the international environment and a state’s perception of international relations and geopolitical environments. Collaboration with platforms and data sharing can enhance cooperation with foreign states, facilitating the free exchange and secure flow of data without restrictive conditions. However, it can also potentially expose a state to vulnerabilities by bolstering the material and innovative capabilities of other countries, thus creating an asymmetrical power dynamic.

The platforms, particularly foreign entities operating beyond a nation’s domestic jurisdiction, can pose challenges to a country’s domestic security objectives, resulting in negative internal security externality. In contrast, domestic platforms that operate within a state’s jurisdiction are more

⁴⁶(Powers and Jablonski 2015, 50–73) The quality and type of data are crucial factors in the military and national security decision-making process, as opposed to the sheer quantity of data. However, the idea of collaboration between the military and commercial sectors on data raises concerns from a state’s perspective. For instance, such statement in particular: “...[O]perational users remain informed of new data-enabled capabilities from the commercial sector...” (US Department of Defense 2020, 10)

⁴⁷Chachko (2021).

⁴⁸Slaughter Matthew and McCormick (2021).

⁴⁹Tusikov (2017); Tusikov (2021).

⁵⁰Zuboff (2019).

⁵¹Tyson and Zysman (1983), 39.

⁵²Rød and Weidmann (2015); MacKinnon (2011).

manageable for governments to control and influence.⁵³ Consequently, certain states may impose their domestic security requirements such as data localization on foreign platforms or assert their sovereign power over cyberspace as a means to counter the influence of these penetrated platforms. This discussion on digital sovereignty reflects the national efforts to safeguard the independent and monopolistic power of states, although it may also provide justification for censorship and surveillance activities by governments.⁵⁴ It is also worth noting that internal security externality can be particularly relevant in the context of authoritarian regimes, where such regimes are inclined to maintain control over domestic discourse and information flow. In these cases, governments may harbor concerns about losing control over domestic security, thereby exacerbating internal security externality.⁵⁵

The exchange of data facilitated by platforms or driven by regional demands can give rise to negative internal security externality, particularly when it involves hostile states. In the context of adversarial relationships, the benefits derived from trade with non-allied states can generate negative security externality with the recipient state.⁵⁶ Data plays a crucial role in informing intelligence and national security decisions, although not all data possesses equal value for prediction and analysis purposes.⁵⁷ In the specific context of power competition between an incumbent leading state and a rising state, negative security externality in the military realm arises when two conditions are met: the potential for conflict with the rising power and its advancement of power through technological innovation and acquisition.⁵⁸ Data, in this sense, becomes instrumental in increasing the likelihood of conflict and enhancing the rising power's capabilities. The issue of data localization—magnified by the claim on digital sovereignty—in turn serves as a balancing measure to address the security threats emanating from external environment, aligning with the discussions surrounding “mercantile realism” and how states balance against each other in economic and technological realms.⁵⁹

Figure 1 encapsulates the underlying mechanism of data localization, which involves domestic users generating data within platforms. This data contributes to the positive network effect, resulting in increased value and gains. Consequently, both network perception and security externality emerge as significant factors influencing the decision to implement data localization. In order for data localization to occur, both negative network perception and negative security externality must be present as a necessary condition. It is significant to recognize the intertwined nature of security and economic aspects within data localization, as no single variable can fully explain its occurrence. A complete explanation for why states pursue data localization over numerous other policy options cannot be solely derived from either network perception or security externality alone. Negative network perception arises when a state perceives dependence, vulnerability, and an inability to benefit from its platform market. On the other hand, negative security externality arises when platforms are seen as hindering domestic affairs (internal) or exposing the nation to security threats from external actors (external). For security externality to have an impact on data localization, either internal security, external security, or both are necessary. Moreover, the prevalence of foreign platforms further amplifies the negative impact of both network perception and security externality. It is this negativity that drives states to strategically implement data localization measures.

Case selection

The selection of Singapore, Vietnam, and Indonesia as case studies is based on their similar geographical location and market characteristics. In order for states to effectively leverage their domestically produced data with platforms, it is essential for them to have a large number of internet users and a sizable platform market.⁶⁰ Platforms are unlikely to find a state with a small user base

⁵³Zhang and Mitchell (2022).

⁵⁴Mueller (2020), 791–793; Christakis (2020), 5–8.

⁵⁵Wu (July, 2021); Sargsyan (2016).

⁵⁶Gowa and Mansfield (1993); Mastanduno (1991).

⁵⁷Van Puyvelde, Coulthart, and Hossain (2017).

⁵⁸Kennedy and Lim (2018), 558.

⁵⁹Heginbotham and Samuels (1998).

⁶⁰Drezner (2008), 5.

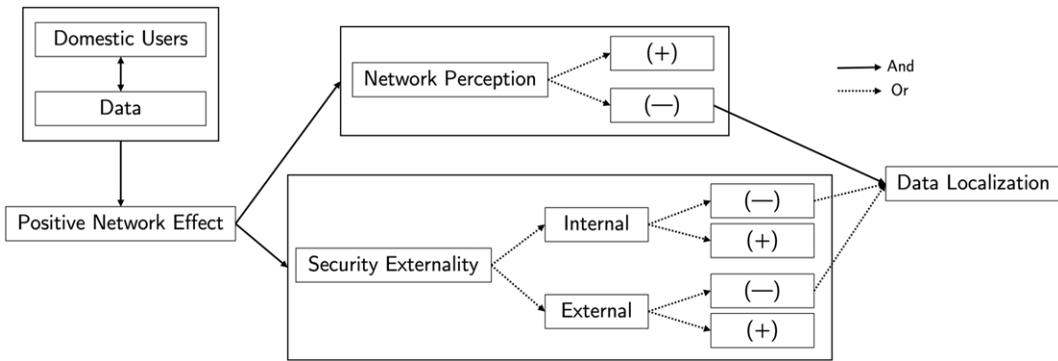


Figure 1. Theoretical mechanism.

attractive for market penetration. In Southeast Asia, where the digital, internet services, and platform markets are experiencing exponential growth,⁶¹ Singapore, Vietnam, and Indonesia exemplify this trend.

The three countries (Table 1) also provide variations in terms of their approach to data localization. Vietnam was the first to introduce data localization measures in 2012, while Singapore does not have explicit data localization requirements. Indonesia initially implemented data localization in 2012, similar to Vietnam, but later revoked it in 2019. Furthermore, Singapore stands out for its well-established digital infrastructure, positioning it as a more advanced digital economy. However, according to the Digital Intelligence Index, both Vietnam and Indonesia exhibit potential for further development, presenting comparable conditions to Singapore.⁶² Thus, the cases of Vietnam, Singapore, and Indonesia offer insights into both cross-country and within-country variations in data localization practices.

Based on the binary approach of data localization, Vietnam and Indonesia with data localization are expected to exhibit negative network perception and security externality. On the other hand, Singapore and Indonesia without data localization are anticipated to demonstrate positive network perception and security externality. Although Singapore ostensibly prohibits the transfer of personal data outside its jurisdiction, this case further supports the notion that states consider various factors, including their own strategic interests and perceptions, when making decisions related to data localization. As the further section will discuss, Singapore’s actual implementation of these regulations nevertheless reflects a strategic pursuit of promoting the free flow of data rather than strict data localization. In addition to its role as a regional digital hub, Singapore strategically chooses to avoid data localization measures. The case of Singapore emphasizes the importance of the perceptual aspect in understanding data localization decisions.

The case study highlights the significant role of network perception and security externality in relation to US platforms, and by extension, the US per se. The affiliation or headquarters of a platform further amplifies the impact of network perception and security externality. When a foreign platform dominates the market in a particular state, it becomes challenging for that state to fully exploit the benefits gained by the platform, particularly if the platform is under the jurisdiction of a hostile country.⁶³ Figure 2 illustrates the global landscape of platform popularity, revealing a clear predominance of US platforms. Out of the top 15 platforms, eight are US companies, while the remaining six Chinese platforms are primarily popular within their domestic market and have limited global influence, which makes China a unique case. This dominance of US platforms poses a challenge

⁶¹World Bank (2021), 103–188.

⁶²Digital Intelligence Index (2020).

⁶³Abraham Newman and Posner (2011), 591–593.

Table 1: Case observation

	Vietnam	Singapore	Indonesia	
			GR82 (2012)	GR71 (2019)
Data Localization	O	X	O	X
Network Perception	(-)	(+)	(-)	(+)
Security Externality	(-) Internal	(+)	(-) Internal	(-) Internal & External

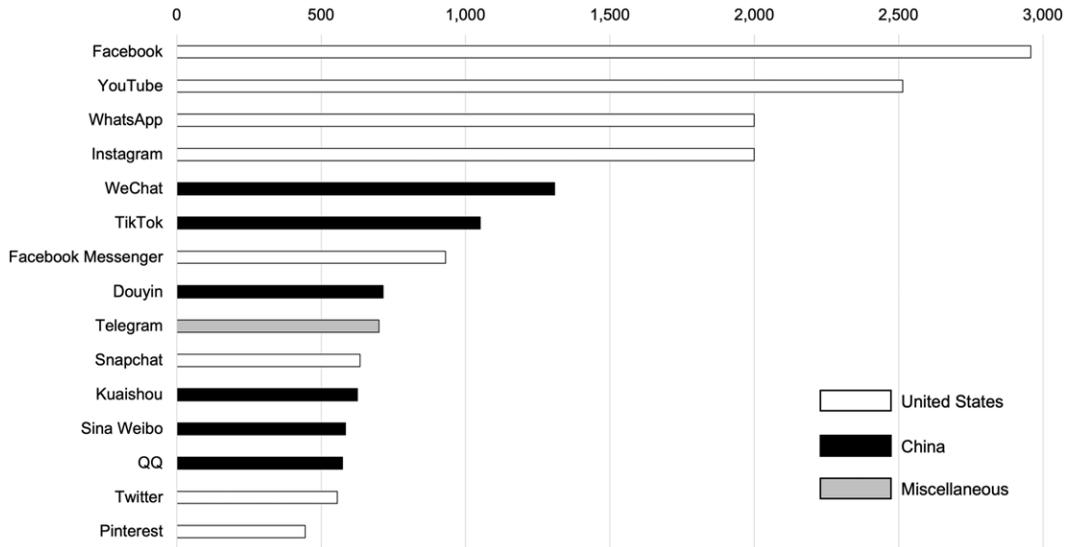


Figure 2. Most popular social networks as of January 2023 (monthly active users in millions).
 Source: Statista, <https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users>

for users who seek to circumvent their influence, despite the multi-homing effect where users may engage with multiple platforms rather than remaining loyal to a single one.⁶⁴

The comparative case study conducted in this paper adopts a process-tracing methodology, which involves the careful selection of specific cases to establish and substantiate the causal mechanism underlying data localization.⁶⁵ Process-tracing is a qualitative approach that leverages contextual evidence to identify the key factors influencing the desired outcome.⁶⁶ In addition to secondary sources, this paper examines contextual evidence from various government-published documents, ministerial and diplomatic statements, press releases, media interviews with senior-level officials, and opinion submissions to international bodies. By incorporating these primary sources of information, the research ensures a thorough examination of the relevant contexts and perspectives surrounding the issue of data localization and statecraft. Employing process-tracing in conjunction with comparative analysis, this study effectively combines empirical analysis of the selected cases with theoretical propositions derived from observing the causal process.⁶⁷ This integrated approach provides a robust framework for examining the intricate interplay between variables within the realm of data localization and statecraft.

⁶⁴Zhu and Iansiti (2019).

⁶⁵Bennett and Elman (2006), 460–463; Mahoney (2007); Seawright and Gerring (2008).

⁶⁶Trampusch and Palier (2016); Waldner (2015); Lorentzen, Fravel, and Paine (2017).

⁶⁷Levy (2008).

Case study

Vietnam

Negative network perception

The history of data localization in Vietnam dates back to Decree 72 (Decree No. 72/2013/ND-CP of July 15, 2013) in 2013 and its amendments in 2018. Decree 73 stipulates that social network entities have at least one server system in Vietnam. Moreover, entities which utilize Vietnamese information facilities or have at least one million monthly internet users have to establish a branch in Vietnam in addition to storing data locally. The first cybersecurity law in 2018 consolidates regulatory regimes, which delineates the type of data entities should store and of entities subject to this law albeit still equivocally defined. A significant development in the context of data localization is the issuance of Decree 53 (Decree 53/2022/ND-CP) in August 2022. This decree serves as a supplement to the existing cybersecurity law and provides further clarification regarding the obligation of foreign entities to store data locally.⁶⁸ Specifically, Article 26 of the Decree stipulates that both domestic enterprises and nearly all internet and digital-related foreign services are required to maintain local data storage.

Vietnam recognizes the significant role of the network effect in platform business and seizes the opportunity it presents. The Vietnamese government has approved the National Strategy on the Development of the Digital Economy and Digital Society to 2025 (Decision No. 411/QĐ-TTg 2022). This strategy highlights the importance of data as the “lifeblood of the digital economy and digital society” and identifies digital platforms as essential “soft infrastructure.”⁶⁹ Building on this strategy, it aims to leverage national digital platforms to provide more tailored services and cater to specific demands from Vietnamese users. Consequently, the strategy emphasizes the need for the swift completion of a legal framework on data and data governance.⁷⁰ However, Hanoi’s approach to data localization is not hasty. Deputy Minister of Information and Communications (MIC), Nguyen Huy Dung, emphasizes the importance of data sharing being in compliance with domestic regulations and laws.⁷¹ This cautious approach reflects Vietnam’s commitment to striking a balance between harnessing the benefits of data and ensuring adherence to regulatory frameworks.

Data localization serves as a strategic interest for Vietnam, driven by the goal of internalizing benefits and promoting national development. The introduction of Circular 38/2016/TT-BTTTT by MIC demarcates the boundaries for foreign entities operating in Vietnam and mandates compliance with Vietnamese legislation.⁷² In a similar vein, the scope of the third draft version of the Cybersecurity Administrative Sanctions Decree encompasses foreign platforms and internet services, subjecting them to monetary penalties.⁷³ These recent regulations demonstrates the vulnerability posed by foreign platforms and aims to level the playing field. The MIC report highlights the significant revenue disparity, with foreign platforms generating \$370 million compared to the largest local platform’s earnings of \$7 million.⁷⁴ In line with data localization efforts, the implementation of physical infrastructure, including local offices and data storage facilities, creates additional hurdles for foreign platforms, acting as barriers to their business activities. The recent issuance of Decree 53 has prompted platforms like Google and Facebook to contemplate their response to the sweeping data regulations

⁶⁸Enterprises established by or registered under foreign law in the following sectors: Telecommunications services, storing and sharing of data in the cyberspace, providing national or international domain names for service users in Vietnam, e-commerce, online payment, payment intermediary, services of connection and transportation in the cyberspace, social media and social communication, online games, and services of providing, managing, or operating other information in the cyberspace in forms of messages, calls, video calls, emails, and online chatting.(Vy October, 2022)

⁶⁹National Academy of Public Administration (March 31, 2022).

⁷⁰National Academy of Public Administration (March 31, 2022).

⁷¹Ministry of Information and Communications (November 17, 2021).

⁷²Foreign information services “that rent digital information storages in Vietnam to provide services, or have a number of visits from Vietnam of one million or higher in one month” come under it.(Ministry of Information and Communications December 26, 2016)

⁷³Massmann (June 7, 2023).

⁷⁴Mai (September 8, 2018).

imposed by the Vietnamese government.⁷⁵ Consequently, business interest groups have raised objections, criticizing the extraterritorial jurisdiction imposed on foreign-headquartered platforms and calling for the revocation of such measures.⁷⁶

Data localization in Vietnam not only serves the strategic interest of internalizing benefits but also empowers domestic platforms to capitalize on positive network effects. The platform market in Vietnam is dominated by Facebook and Zalo holding over 90 percent of the market share.⁷⁷ The recently approved National Cybersecurity and Safety Strategy (Decision 964/QĐ-TTg) underscores the importance of developing endogenous platforms in Vietnam. It emphasizes the need to create a digital platform that is utilized by both Vietnamese and international citizens and highlights the capacity for self-reliance to safeguard national sovereignty in cyberspace.⁷⁸ Recognizing the significance of local platforms, the Vietnamese government has set a target of having 50 percent of local users using domestic platforms by 2030. Zalo, along with two other domestic platforms, is identified as a major player in the country's domestic platform ecosystem.⁷⁹

Negative security externality: internal

When examining security externality, the focus of Hanoi's analysis lies primarily on negative internal externality rather than external factors. The main concern revolves around the potential loss of control by the Vietnamese Communist Party in the digital realm. This is evident in various cybersecurity-related decrees, regulations, and strategies, all of which emphasize the significant role of the Party. The Cybersecurity and Safety Strategy, for instance, prioritizes "Strengthening the leadership of the Party and management of the State over cybersecurity" as a top priority in the strategy.⁸⁰ Additionally, Decree 13/2023/ND-CP on personal data protection places a greater emphasis on the involvement of the Ministry of Public Security, requiring entities to notify the Ministry for cross-border data flows.⁸¹ These actions collectively demonstrate Hanoi's concern for internal security and the consequential negative internal security externality it perceives.

Vietnam has a history of suppressing internet freedom and implementing internet censorship since the early days of the internet. The country's cybersecurity definition places importance on preventing activities that could harm social order and safety, with party leadership as the top priority. However, despite its Communist Party system, Vietnam's regulatory environment for data localization shares similarities with other states, distinguishing it from other communist countries that aim for complete control and prohibition of non-conforming foreign entities. Vietnam acknowledges the conflict between communist values and the development of the digital economy, demonstrating an awareness of the limitations of its regulatory approach.

Vietnam understands the challenges of completely rejecting foreign platforms and the potential diplomatic issues that may arise by recognizing that it is neither desirable nor feasible to ban all foreign platforms or impose oppressive censorship measures.⁸² Furthermore, Vietnam is a rapidly growing digital market, with a digital economy valued at approximately \$14 billion in 2020 and projected to experience 30 percent growth until 2025.⁸³ Sustaining this growth solely through endogenous efforts is challenging. Additionally, Vietnam's regulatory environment in the ICT sector is evolving, recognizing the significance of foreign investment. Regulatory data shows a shift from the most restrictive G1 group

⁷⁵P. Nguyen (August 18, 2021).

⁷⁶American Chamber of Commerce in Vietnam (September, 2022); "BSA Comments on Proposed Amendments to Draft Decree 72" (September 3, 2021).

⁷⁷The specific platform business structure is as follows: Facebook (93.8%), Zalo (91.3%), TikTok (75.4%), Instagram (59.7%), and Twitter (34.4%). Depending on sources, some argue that Zalo has more users than Facebook, making it the primary social platform in Vietnam, but these figures are drawn from the above source. (Digital Business Lab July 27, 2022).

⁷⁸*Approval for National Circular Safety and Security Strategy, Actively Responding to Challenges* (2022).

⁷⁹Pearson and Vu (November 8, 2018).

⁸⁰Dung (August 22, 2022).

⁸¹Vietnam Government (April 23, 2023).

⁸²Hiep (2019).

⁸³Huynh (September 20, 2021).

to the more inclusive G3 group, which promotes competition in services and implements measures to protect against public monopolies in regulation.⁸⁴ This improvement reflects Vietnam's efforts to develop its regulatory framework and create an environment conducive to attracting foreign investors.

Vietnam's motivation for data localization is primarily driven by internal security concerns, rather than external security considerations. The Vietnamese Communist Party seeks to maintain control and restrict the flow of domestic information, which amplifies the demand for data localization alongside the network externality. This is evident through a range of policies aimed at controlling the domestic flow of information, as well as the cooperative relationship between the Vietnamese technology conglomerate and the Communist Party, which serves internal security interests.⁸⁵ While Vietnam recognizes the importance of market competitiveness in the digital economy, the internal purpose of data localization and the government's intention to utilize it to serve its own interests remain decisive factors. However, the influence of external security considerations on data localization is relatively limited, considering the dominant position of US platforms in Vietnam compared to the limited influence of Chinese platforms. It is worth noting that Vietnam's cooperation with the United States has evolved due to increased Chinese assertiveness in the region, given Vietnam's tenuous relationship with China.⁸⁶

Singapore

Positive network perception

Singapore's data regulations have evolved since the introduction of its first data protection law in 2012, known as the Personal Data Protection Act of 2012 (No. 26 of 2012, PDPA). Section 26 of the PDPA, known as the Transfer Limitation Obligation, outlines the conditions for transferring personal data outside of Singapore. Unlike data localization approaches, Singapore allows data transfer under certain conditions without imposing restrictions on local data storage or processing. Subsequently, significant updates to data-related regulations were implemented after 2020, including the introduction of the Personal Data Protection Regulation 2021. This new regulation, enacted in 2021, provides further clarification on the conditions under which data transfers are permitted. Under this framework, the transferring entity bears the responsibility of ensuring that the foreign data recipient maintains comparable protection measures to those in Singapore. Furthermore, an amendment to the PDPA was introduced in November 2020 to strengthen user rights and enhance the accountability of entities handling personal data. This amendment emphasizes users' rights to inspect the usage of their data and aims to improve the responsibility of data-handling entities, while also seeking more effective enforcement mechanisms.

Singapore recognizes the potential of the platform ecosystem and aims to leverage its benefits for economic development. Similar to the Vietnamese market structure, where US platforms dominate without strong endogenous platforms,⁸⁷ the Singapore government seeks to establish an accountable and robust foundation for platforms, enabling "the legitimate use of data."⁸⁸ In Singapore, the fundamental principle underlying data regulation is accountability, wherein organizations are held responsible for the data under their possession or control.⁸⁹ This principle fosters a trustworthy environment where platforms in Singapore embrace private-led responsibility, rather than relying solely on government-led initiatives. By promoting accountability, Singapore aims to create a conducive environment for platforms to thrive and contribute to economic growth.

Although Singapore does not impose a legally binding requirement for data localization, the data transfer restrictions outlined in the PDPA can be seen as a form of data localization in a different

⁸⁴International Telecommunication Union (n.d.).

⁸⁵Potkin and P. Nguyen (September 28, 2022); Luong (2022).

⁸⁶Grossman and Sharman (December 31, 2019); Tu and H. T. T. Nguyen (2019).

⁸⁷The specific platform market share is as follows: Whatsapp (83.7%), Facebook (79.4%), Instagram (66.3%), Telegram (49.2%), and TikTok (44.3%).(Hootsuite February 14, 2022).

⁸⁸Teo (March 4, 2022), 122.

⁸⁹Singapore Government (December 21, 2022).

format. The “raison d’être” of the Transfer Limitation Obligation is to safeguard personal data in Singapore from foreign entities over which Singapore has limited jurisdiction and sovereign power.⁹⁰ However, the implementation of the Transfer Limitation Obligation is done in a limited and flexible manner to promote the development of the digital economy. For instance, Singapore has chosen to recognize the Asia Pacific Economic Cooperation’s Cross-Border Privacy Rules (CBPR) and Privacy Recognition for Processors (PRP) programs as legally equivalent to its PDPA. This recognition exempts member states of the PRP program from the Transfer Limitation Obligation. The condition for cross-border data transfer, as specified in the article, is simplified as a requirement for reciprocal and equivalent measures to PDPA. This provision highlights Singapore’s strategic decision to provide support and establish a reliable foundation based on the perceived reliability of the entities themselves. By adopting this approach, Singapore aims to facilitate the smooth flow of data while maintaining strong data protection standards.

Singapore has positioned itself as a frontrunner in promoting cross-border data transfers and views it as an opportunity rather than a vulnerability. The national strategy known as Smart Nation Singapore, which focuses on harnessing technologies, emphasizes the role of digitalization as a driver for economic growth and societal transformation. Within this strategy, data is recognized as a fundamental asset that is essential for achieving exponential growth in the digital economy. “Singapore’s data protection ecosystem facilitates an increase in data sharing activities . . . for the increased competitiveness of Singapore’s economy.”⁹¹ Josephine Teo, the Minister for Communications and Information, highlights the importance of international cross-border data flows as “The free flow of data across borders enables our business to digitally serve many markets, creating efficiencies and driving innovation.”⁹² She further underscores the challenges businesses face when operating in multiple jurisdictions, stating that it would be impractical to meet all the requirements of different jurisdictions while maintaining efficient business operations.⁹³ By promoting the free flow of data across borders, Singapore aims to create an environment that supports seamless business operations and fosters innovation.

In tandem with all the endeavors, Singapore actively promotes the principle of the free flow of data internationally under the principle of “choose where they can store their data.”⁹⁴ As a founding state of Digital Economy Partnership Agreement (DEPA), it accentuates cross-border data flows and aims to enhance connectivity and promote a free and open internet environment. Given Singapore’s position as a central node in the international flow of data, DEPA aligns with the goal of prohibiting data localization and promoting interoperability of outbound data transfers in accordance with the PDPA.⁹⁵ At the same time, DEPA upholds the concept of enabling the free cross-border transfer of data while recognizing the need for regulatory measures. It also discourages arbitrary and unjustifiable demands for computing facilities in foreign territories as a condition for conducting business. This approach is consistent with Singapore’s recent digital partnership with the European Union and the Memorandum of Understanding on data cooperation with the United Kingdom.⁹⁶

Positive security externality

Singapore’s approach to data localization distinguishes it from countries characterized by negative internal and external security externalities. Singapore, as a democratic nation, does not emphasize internal security externality. Instead, it has established the Personal Data Protection Commission (PDPC) under the Personal Data Protection Act (PDPA) to safeguard personal data and enforce data protection obligations on businesses. Unlike Vietnam, there is no explicit emphasis on government

⁹⁰Personal Data Protection Commission (2022).

⁹¹Infocomm Media Development Authority (2017), 32.

⁹²Teo (December 1, 2022).

⁹³Teo (April 5, 2023).

⁹⁴Ministry of Trade and Industry (2023a).

⁹⁵Iswaran (November 2, 2020).

⁹⁶Ministry of Trade and Industry (2023b); Ministry of Communications and Information (June 27, 2023).

control over platforms and markets. The regulatory framework places the responsibility for data protection on private entities, reducing the need for state surveillance and enhancing Singapore's appeal as a favorable location for data-related business activities. On the other hand, as a result of its market structure, with dominant US platforms, Singapore prioritizes cooperation on data transfer with the United States and actively seeks partnerships with like-minded countries. In this regard, Singapore has established individual digital economy agreements with three states, demonstrating its commitment to fostering collaborative coalitions in the digital realm.

As an early mover in Asia, Singapore entered into a free trade agreement with the United States that included a "groundbreaking" e-commerce section.⁹⁷ This section serves as a model for other trade agreements by establishing principles of nondiscrimination and the prohibition of duties on e-commerce services and items. The cooperative relationship between Singapore and the United States has expanded to encompass data cooperation in sensitive areas such as financial services. Both countries have committed to "oppose generally applicable data localization requirements."⁹⁸ In a more recent development, Singapore and the United States have initiated a Partnership for Growth and Innovation (PGI), which prioritizes the free flow of data as part of Singapore's Smart Nation strategy. This partnership further underscores the commitment of both countries to facilitate the movement of data across borders for the benefit of economic growth and innovation.⁹⁹

Singapore actively promotes an open and secure international environment for data transfer, focusing on international partnerships beyond its ASEAN counterparts. The country's cybersecurity strategy, particularly the second strategy published in 2021, emphasizes the cultivation of such an environment. Singapore takes proactive measures to advocate for the free flow of data in various international forums. Notably, it has established the Global Cross-Border Privacy Rules (CBPR) forum in collaboration with six other countries. All member countries of the CBPR forum recognize the importance of trusted cross-border data flows and believe that such flows contribute to improving lives.¹⁰⁰ Additionally, Singapore, the United States, and Japan are leading the Joint Initiative on e-commerce within the World Trade Organization, with the goal of promoting free and secure data transfer.¹⁰¹ These efforts highlight Singapore's commitment to creating a conducive global environment for the exchange of data.

Indonesia

Negative network perception

In 2012, Indonesia introduced data localization requirements through Government Regulation No. 82 (GR 82) without providing a clear definition. GR 82 forces "operator for the public service" to build "the data center and disaster recovery center in Indonesia territory for the purpose of . . . enforcement of national sovereignty to the data of its citizen."¹⁰² Despite this ambiguity surrounding the definition, Indonesia had implemented such data localization since 2012. The Minister of Communication and Informatics (MCIT) emphasized the significance of data localization for law enforcement purposes, noting that "if the data centers are located overseas . . . [law] enforcers cannot gain physical access."¹⁰³ Consequently, the Indonesian government urged foreign service providers like Google and BlackBerry to store data locally, highlighting the construction of a data center in Indonesia as the remaining requirement.¹⁰⁴

Indonesia's adoption of a stringent data localization policy can be attributed to its aspirations for sovereignty and independence, primarily due to the country's heavy reliance on foreign platform

⁹⁷Pang (2011), 83.

⁹⁸US Department of Treasury (February 5, 2020).

⁹⁹US Department of Commerce (October 27, 2022).

¹⁰⁰US Department of Commerce (April 22, 2022).

¹⁰¹Suneja (May 4, 2018).

¹⁰²Government (October 12, 2012); Ministry of Communication and Informatics (December 1, 2016).

¹⁰³Bhaskoro (May 8, 2013).

¹⁰⁴Dewan (December 11, 2011); Ministry of Communication and Informatics (December 18, 2011).

firms.¹⁰⁵ The MCIT criticizes foreign entities such as Google and Facebook for extracting revenues from the Indonesian population without reciprocating in a fair manner.¹⁰⁶ The Defense White Paper of 2008 highlights Indonesia's dependence on foreign products and technologies, which raises concerns about potential technological threats and the erosion of Indonesia's position in the global landscape.¹⁰⁷ The 2015 Defense White Paper reiterates this concern and underscores the importance of economic independence by advocating for the development of strategic sectors within the domestic economy.¹⁰⁸ These assessments indicate that Indonesia perceives the dominance of foreign platforms in its market as a negative network perception that could compromise its autonomy and national interests.

Positive network perception

The Indonesian government has undergone a shift in its stance on data localization, as reflected in the implementation of new regulations and laws. Government Regulation No. 71 (GR 71), introduced in 2019, replaced the previous regulation (GR 82) and provided clearer definitions regarding data localization. GR 71 distinguishes between the public and private domains, categorizing entities related to the government or governmental agencies as part of the public domain, while private entities providing electronic services to the public fall under the private domain. As a result, different standards are applied, whereby service providers in the public domain are still obligated to localize data, while private providers, with the exception of financial data, are no longer required to adhere to localization measures.¹⁰⁹ This change provided a more precise framework for data localization in Indonesia.

Furthermore, the enactment of the Personal Data Protection Law (PDPL) in 2022 marks a significant milestone in Indonesia's data transfer process. This law is expected to facilitate data transfers between countries, albeit with the requirement that the recipient countries offer data protection measures that are equivalent to those outlined in Singapore's regulations. While the PDPL retains the need for compliance with cross-border data transmission requirements, it ensures a secure transfer as long as the recipient countries provide adequate data protection measures in line with Singapore's standards.¹¹⁰ The PDPL signifies a new era in data protection legislation in Indonesia and is anticipated to streamline the data transfer process while maintaining data security.¹¹¹

The prevalent perception in Indonesia now leans towards maximizing the benefits derived from foreign platforms, leading to a rescindment of data localization. The significant contribution of the digital economy sector, which attracts approximately 10 percent of foreign investment annually (around \$20-25 billion), has shifted the perception of dominant foreign platforms in Indonesia from a vulnerability to an opportunity for developing the country's digital infrastructure and economy.¹¹² Recognizing the importance of developing its own digital economy and infrastructure, the Indonesian government introduced its first e-commerce roadmap in 2016, aiming to create a "safe and open" e-commerce industry. The roadmap acknowledged the significance of learning from advanced e-commerce countries such as China and the United States to advance Indonesia's national e-commerce sector.¹¹³ It positioned e-commerce as a crucial component of the national economy and identified it as a "backbone of the national economy."¹¹⁴

In line with the Making Indonesia 4.0 strategy in 2018 emphasizing inclusive digital infrastructure, the recently unveiled 2021-2024 Digital Indonesia roadmap, highlighted by Minister of

¹⁰⁵The total market share of Facebook, Twitter, and Youtube has marked 90 percent since 2009. Facebook initially had about 80 percent of the market share, whereas its share is replaced by Twitter and Youtube leading to steady foreign dominance in Indonesia. (GLocalStats February, 2023)

¹⁰⁶Ministry of Communication and Informatics (March 15, 2016).

¹⁰⁷This is cited from (Priyandita, Kley, and Herscovitch 2022, 19), originally from (Ministry of Defence 2008, 38).

¹⁰⁸Ministry of Defence (2015), 39.

¹⁰⁹PwC (November, 2019).

¹¹⁰Dorwart et al. (October 19, 2022).

¹¹¹Widianto (September 20, 2022).

¹¹²Ministry of Communication and Informatics (March 11, 2019).

¹¹³e-Commerce Association of Indonesia (January 14, 2016).

¹¹⁴Ministry of Law and Human Rights (August 3, 2017), 2.

Communication and Informatics Johnny Plate, also underscores the importance of inclusive digital infrastructure to expedite Indonesia's transformation in the digital economy and trade sector.¹¹⁵ Indonesia acknowledges that restrictions on cross-border data flows present obstacles to its development.¹¹⁶ In various negotiation and analytical documents, including those released by governments, Indonesia's efforts to eliminate data localization measures are evident. By promoting unencumbered data transfer, Indonesia aims to stimulate economic development for service providers and attract more investors.¹¹⁷ In a similar vein, Indonesia has designated the digital economy as one of the strategic pillars during its ASEAN chairmanship in 2023, emphasizing its commitment to creating a favorable environment for foreign investment.¹¹⁸ These initiatives collectively reflect Indonesia's determination to leverage the opportunities presented by foreign platforms and cross-border data flows to foster economic growth and development.

Negative security externality: internal

Indonesia's notion of security is grounded in the integrity of a single nation due to its historic vulnerability and diverse cultural heritage. The country's perception of national security is linked to data localization, which is deemed crucial for national integrity. The national law on electronic information and transaction (No. 11 of 2008) emphasizes the importance of supporting "religious and social-cultural values of the Indonesian society," maintaining national unity, and protecting the nation's dignity, degree, and sovereignty.¹¹⁹ This law is supported by the MCIT regulation, which mandates that wireless broadband service providers include a proportion of local content of up to 50 percent.¹²⁰ The enforcement of data localization serves as a measure to exert national regulatory power over foreign entities and protect national integrity by addressing internal security concerns. The secessionist movement that emerged after Timore-Leste's referendum in 1999 has been a primary domestic security concern. During Yudhoyono's presidency from 2004 to 2014, securing internal security to tackle separatist actions became a policy priority, and his efforts led to successes such as the Helsinki agreement on the Aceh region.¹²¹

Compared to internal security externality, there is little evidence that negative external security results in data localization before GR 71 promulgates. Yudhoyono administration pursues a "zero enemies, a million friends" stance in tandem with "dynamic equilibrium" where Indonesia takes centrality within the ASEAN to prevent external powers and promote regional cooperation.¹²² His national strategy supports a robust relationship with the United States with the successful consolidation of democracy in Indonesia. It elevates the bilateral relationship to Comprehensive Partnership in 2010 and both defense ministers pledges to foster defense cooperation from maritime to global threats. After President Jokowi takes the office, Indonesia displays a robust relationship with the United States by highlighting both regional and global cooperation in various areas while distancing from China. Indonesian Foreign Minister evaluates US commitment to the region and Indonesia as "very noticeable" in the midst of increasing tension with China, demonstrating a robust and positive security externality.¹²³

Negative security externality: internal and external

The security externality in Singapore is further augmented by negative external security externality resulting from reciprocity between states, in addition to the existing negative internal one. Even after

¹¹⁵Ministry of Industry (2018); Putri and Ruhman (March 23, 2022).

¹¹⁶Ministry of Trade (2021), 101–102.

¹¹⁷Department of Foreign Affairs and Trade (2019), 14.

¹¹⁸Presidential Staff Office (March 9, 2023).

¹¹⁹Ministry of Law and Human Rights (April 21, 2008).

¹²⁰US Trade Representative (April 2013), 20.

¹²¹Jones (2015).

¹²²Ciorciari (2018).

¹²³Pamuk and Widiyanto (December 13, 2021).

the inauguration of the Jokowi administration, which expanded foreign policy to encompass more diverse agendas, the internal security driver remains significant. The government of Indonesia prioritizes regulating platform businesses to safeguard digital sovereignty and protect the state from “negative contents that can destroy unity and ruin national digital sovereignty.”¹²⁴ The implementation of the PDPL is seen as an opportunity to “strengthen the role and authority of the government” in data governance.¹²⁵ The temporary interdiction on foreign platforms reflect the government’s commitment to safeguarding the public from disruptive online content.¹²⁶ Indonesia recognizes that data is intertwined with national sovereignty and geopolitical interests, prompting a consideration of the structural aspects and geopolitical ramification of data localization.¹²⁷ In contrast to the 2019 G20 Summit, Indonesia expands the scope of its agenda to encompass cross-border data flows, emphasizing the principle of reciprocity. By advocating for interoperability and appropriate policy measures in cross-border data flows, Indonesia’s actions highlight the negative external security externality generated by the international and geopolitical environment surrounding data and digital trade.

Despite outweighed positive network perception leading to abolishing data localization concerns regarding asymmetry with foreign platforms linger. Officials have highlighted the reliance of Indonesians on foreign platforms and the advantages enjoyed by companies “who are far away there.”¹²⁸ This perception underscores the need for greater data sovereignty and control. For instance, a senior official in the ministerial coordinating group said, “If you have a nationalist spirit, then move your data to Indonesia.”¹²⁹ The enactment of PDPL is viewed as an attempt to establish a virtual border that safeguards individual rights and protects data sovereignty.¹³⁰ The National Strategy for AI envisions a prosperous Indonesia in 2045 driven by “the sovereignty of Indonesian data for the benefit of Indonesia,” ensuring that it is not controlled by foreign entities.¹³¹ In the context of international discussions, Indonesia underscores the principles of sovereignty and data security. During the G20 Summit, Minister Plate affirmed Indonesia’s commitment to these principles and proposed the inclusion of lawfulness, fairness, and transparency as guiding principles for data flows.¹³² This approach reflects Indonesia’s aspiration to exercise sovereign power over its data while advocating for reciprocal guarantees of free data flow from other nations. The aim is to strike a balance between safeguarding national interests and promoting international cooperation in data governance.

Indonesia’s approach to data localization as a result demonstrates a cautious balance between internal integrity, international reciprocity, and digital sovereignty. As Minister Plate claims, “Data sovereignty is important so that the movement of values and data flows both nationally and globally can be managed properly.”¹³³ He positions Indonesian digital sovereignty as “the third phase in Indonesia’s struggle,” following its struggle for decolonization and the establishment of its archipelagic state identity.¹³⁴ This consistent message highlights Indonesia’s considerations of both internal and external security factors. The Digital Economy Minister’s report during Indonesia’s presidency in 2022 further exemplifies the disparity between positive network perception and negative security externality. While acknowledging the role of free data flows as a key driver for economic growth and development, Indonesia simultaneously incorporates the concepts of the free flow of data across borders and data sovereignty.¹³⁵ Similarly, the National Strategy for AI outlines practical implementations of data localization and provides explicit guidelines for data sharing practices.¹³⁶

¹²⁴K. and Ruhman (August 17, 2022).

¹²⁵Ministry of Communication and Informatics (September 20, 2022).

¹²⁶Mulyanto and Galuh (August 4, 2022).

¹²⁷A. and Ruhman (June 18, 2022).

¹²⁸Coordinating Ministry for Political, Legal and Security Affairs (December 9, 2022).

¹²⁹Presidential Staff Office (October 26, 2022).

¹³⁰Mawangi and T. (July 22, 2021).

¹³¹Technology Assessment and Assessment Agency (BPPT) (2020), 14.

¹³²Ministry of Communication and Informatics (July 23, 2020).

¹³³Ministry of Communication and Informatics (August 17, 2022).

¹³⁴Ministry of Communication and Informatics (March 22, 2022).

¹³⁵Plate (2022), 5.

¹³⁶Technology Assessment and Assessment Agency (BPPT) (2020), 51.

Conclusion

The complex relationship between states and the various dimensions of data, including individual referents, platforms, and structural characteristics, highlights the limitations of a singular and discrete approach in understanding states' motivations for data localization. Instead, data localization should be viewed as a strategic decision by states to advance their political objectives. This paper argues that data localization is a form of economic statecraft that arises from the intersection of digital technology, proposing a nuanced mechanism that integrates network perception and security externality—both at domestic and international levels. Through an examination of three Southeast Asian states, it asserts that data localization is driven by a state's comprehensive understanding of the network effect, rather than being influenced by a single factor. Specifically, the state's perspective on the economic impact and security implications of data localization is crucial. The decision of states to implement data localization finds a comprehensive explanation only through the synergy of both network perception and security externality—rather than reliance on either alone. This comprehensive perspective is essential, given the array of strategic options available beyond data localization and its interwoven nature within the domains of economy and security.

This paper makes significant contributions to the existing literature in international relations, particularly within the fields of international political economy, international security, and technology. It extends the concept of economic statecraft to encompass the realm of digital technology.¹³⁷ While data has always been present, the recent advancements in digital technologies have transformed its value and generated new opportunities that were previously unimaginable. While traditional concepts and theories in international relations still hold relevance, this paper delves into how data, as the core element of digital technology and AI, operates within the context of economic statecraft.

Furthermore, this paper advances the discussion on the interconnectedness of international political economy and international security. Recognizing that statecraft inherently combines foreign economic and security policies, the development of technology creates new avenues for statecraft to manifest in economic, military, and societal domains.¹³⁸ Drawing from theoretical approaches in both disciplines, this paper emphasizes the necessity of integrating and considering both perspectives in the theoretical mechanism. It highlights that neither perspective alone but both can provide a comprehensive understanding of the complex dynamics at play. After all, data in digital technology serving as a vital resource for training AI is an economic means that emerges from the network effect, comprising both economic aspects and security ramifications.

In practice, data localization is not merely an autonomous decision but a representation of strategic calculation. This understanding is crucial in assessing partners' responses to data localization in bilateral and multilateral relations. For example, the US Trade Representative openly characterizes data localization as a foreign trade barrier.¹³⁹ In order to address the growing number of countries implementing data localization measures, the United States needs to develop a strategy that reframes these measures as opportunities rather than vulnerabilities, while also alleviating security concerns. In other words, the decision to implement data localization not only impacts other states but is also influenced by the policies and strategies of those states vice versa. As a result, this dynamic interplay underscores the need for nuanced and delicate countermeasures in response to data localization.

Acknowledgements. I would like to thank Jon Lindsay, Peter Swire, Milton Mueller, Katharina Fleiner, and Vagisha Srivastava for reading the earlier draft. I am also thankful to Alasdair Young, Ahmed Said, Katharina Kuhn, Hyunsu Kim, participants from the ISA 2023 Virtual Conference, the 22nd Workshop on the Economics of Internet Security (WEIS), the 2023 Cybersecurity Summer Institute, the Graduate Students in International Political Economy (GSIPE) 5th mini-conference, Nunn School Writer's Nest, and IR Salon, as well as anonymous reviewers and the editors at *Business and Politics*.

¹³⁷C. Liu (2023).

¹³⁸Mastanduno (1998); Goddard, MacDonald, and Nexon (2019).

¹³⁹US Trade Representative (2023), 2.

References

- Afuah, Allan. 2013. "Are Network Effects Really All about Size? The Role of Structure and Conduct." *Strategic Management Journal* 34 (3): 257–273.
- Ali, Aran. September 2020. *Here's What Happens Every Minute on the Internet in 2020*. https://www.weforum.org/agenda/2020/09/internet-social-media-downloads-uploads-facebook-twitter-youtube-instagram-tiktok?utm_source=twitter%5C&utm_medium=social_scheduler%5C&utm_term=Internet+of+Things%5C&utm_content=06/10/2020+1430.
- American Chamber of Commerce in Vietnam. September, 2022. "US-ABC's Recommendations – Vietnam's Proposal to Amend Decree 72/2013/ND-CP." In: *American Chamber of Commerce in Vietnam*. <https://www.amchamvietnam.com/wp-content/uploads/2021/09/USABC-AmCham-Submission-on-Decree-72.pdf>.
- Anderson, Ross, and Tyler Moore. 2006. "The Economics of Information Security." *Science* 314 (5799): 610–613.
- Approval for National Circular Safety and Security Strategy, Actively Responding to Challenges. 2022. <https://thuvienphapluat.vn/van-ban/Cong-nghe-thong-tin/Quyết-dinh-964-QĐ-TTg-2022-phe-duyet-Chien-luoc-An-toan-An-ninh-mang-quoc-gia-den-2025-525540.aspx#tab1>.
- Axelrod, Robert, and Robert O. Keohane. 1985. "Achieving Cooperation Under Anarchy: Strategies and Institutions." *World Politics* 38 (1): 226–254.
- Ayoub, Kareem, and Kenneth Payne. 2016. "Strategy in the Age of Artificial Intelligence." *Journal of Strategic Studies* 39 (5–6): 793–819.
- Baldwin, David A. 2020. *Economic Statecraft: New Edition*. Princeton, NJ: Princeton University Press.
- Bamberger, Kenneth A., and Orly Lobel. 2017. "Platform Market Power." *Berkeley Technology Law Journal* 32: 1051–1092.
- Basu, Arindrajit, Elonnai Hickok, and Aditya Singh Chawla. March 19, 2019. "The Localisation Gambit: Unpacking Policy Measures for Sovereign Control of Data in India." *The Centre for Internet and Society*. <https://cis-india.org/internet-governance/resources/the-localisation-gambit.pdf>.
- Bauer, Matthias, et al. 2014. *The Costs of Data Localisation: Friendly Fire on Economic Recovery*. Tech. rep. ECIPE Occasional Paper.
- Beduschi, Ana. 2019. "Digital Identity: Contemporary Challenges for Data Protection, Privacy and Non-Discrimination Rights." *Big Data & Society* 6 (2): 2053951719855091.
- Bennett, Andrew, and Colin Elman. 2006. "Qualitative Research: Recent Developments in Case Study Methods." *Annual Review of Political Science* 9: 455–476.
- Bernal, Paul. 2016. "Data Gathering, Surveillance and Human Rights: Recasting the Debate." *Journal of Cyber Policy* 1 (2): 243–264.
- Bhaskoro, Avi Tejo. May 8, 2013. "Indonesian Ministry Still Insists on Local Data Centers for Online Companies." *DailySocial*. <https://dailysocial.id/post/indonesian-ministry-still-insists-on-local-data-centers-for-online-companies>.
- Bonatti, Alessandro, et al. 2021. "More Competitive Search Through Regulation." *Policy Discussion Paper 2*. <https://tobin.yale.edu/digital-economy-project/policy-discussion-papers>.
- Brander, James. 1988. "Rationales for Strategic Trade and Industrial Policy." In *Strategic Trade Policy and the New International Economics*. Edited by Paul Krugman. Cambridge: The MIT Press, pp. 23–46.
- "BSA Comments on Proposed Amendments to Draft Decree 72". September 3, 2021. *The Software Alliance*. <https://www.bsa.org/files/policy-filings/en09062021dftdecree72.pdf>.
- Buzan, Barry. 2008. *People, States & Fear: An Agenda for International Security Studies in the Post-Cold War Era*. Colchester: ECPR press.
- Bygrave, Lee A. 1998. "Data Protection Pursuant to the Right to Privacy in Human Rights Treaties." *International Journal of Law and Information Technology* 6 (3): 247–284.
- Chachko, Elena. 2021. "National Security by Platform." *Stanford Technology Law Review* 25 (1): 86–94.
- Chaisse, Julien. 2023. "'The Black Pit': Power and Pitfalls of Digital FDI and Cross-Border Data Flows." *World Trade Review* 22 (1): 73–89.
- Chander, Anupam, and Uyên P. Lê. 2015. "Data Nationalism." *Emory Law Journal* 64: 677–739.
- Christakis, Theodore. 2020. *"European Digital Sovereignty": Successfully Navigating Between the 'Brussels Effect' and Europe's Quest for Strategic Autonomy*. Paris: Multidisciplinary Institute on Artificial Intelligence.
- Cioffi, John W., Martin F. Kenney, and John Zysman. 2022. "Platform Power and Regulatory Politics: Polanyi for the Twenty-First Century." *New Political Economy* 27 (5): 820–836.
- Ciorciari, John D. 2018. "Indonesia's Diplomatic and Strategic Position under Yudhoyono." In: *Aspirations with Limitations: Indonesia's Foreign Affairs under Susilo Bambang Yudhoyono*. Edited by Ulla Fionna, Siwage Dharma Negara, and Deasy Simandjuntak. Singapore: ISEAS Publishing, pp. 33–59.
- Confessore, Nicholas. April 2018. *Cambridge Analytica and Facebook: The Scandal and the Fallout So Far*. <https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html>.
- Coordinating Ministry for Political, Legal and Security Affairs. December 9, 2022. "The Importance of Digital Sovereignty through the Independence of Indonesian Social Media Platforms (Pentingnya Kedaulatan Digital Melalui Kemandirian Platform Media Sosial Indonesia)." *Press Release*. 200/SP/H.M.01.02/POLYHUKAM/12/2022. <https://polkam.go.id/pentingnya-kedaulatan-digital-melalui-kemandirian-platform-media-sosial-indonesia/>.

- Cory, Nigel, and Luke Dascoli. July 19, 2021. "How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them." *Information Technology and Innovation Foundation*. <https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost/>.
- Cory, Nigel, Luke Dascoli, and Ian Clay. December 12, 2022. "The Cost of Data Localization Policies in Bangladesh, Hong Kong, Indonesia, Pakistan, and Vietnam." *Information Technology and Innovation Foundation*. <https://itif.org/publications/2022/12/12/the-cost-of-data-localization-policies-in-bangladesh-hong-kong-indonesia-pakistan-and-vietnam/>.
- Crawford, Beverly. 1993. *Economic Vulnerability in International Relations: The Case of East-West Trade, Investment, and Finance*. New York: Columbia University Press.
- Creemers, Rogier. 2022. "China's Emerging Data Protection Framework." *Journal of Cybersecurity* 8 (1): 1–12.
- Cusumano, Michael A., Annabelle Gawer, and David B. Yoffie. 2019. *The Business of Platforms: Strategy in the Age of Digital Competition, Innovation, and Power*. New York: Harper Business New York.
- Department of Foreign Affairs and Trade. 2019. *National Interest Analysis: Category I Treaty*. Barton, MA: Department of Foreign Affairs and Trade. <https://www.dfat.gov.au/sites/default/files/iacepa-1a-national-interest-analysis-including-attachments.pdf>.
- Dewan, Angela. December 11, 2011. "Indonesia Threatens to Cut BlackBerry Data Service." *phys.org*. <https://phys.org/news/2011-12-indonesia-threatens-blackberry.html>.
- Digital Business Lab. July 27, 2022. "Social Media Penetration in Vietnam [Research]." *Digital Business Lab*. <https://digital-business-lab.com/2022/07/27-social-media-penetration-vietnam-research/>.
- Digital Intelligence Index. 2020. "Digital Intelligence Index." *Digital Planet*. <https://digitalintelligence.fletcher.tufts.edu/compare/sg-vn-id/ranking/state/wr>.
- Ding, Jeffrey. 2022. "Dueling Perspectives in AI and U.S.–China Relations: Technonationalism vs. Technoglobalism." In: *The Oxford Handbook of AI Governance*. Edited by Justin Bullock, et al. Oxford: Oxford University Press. <https://academic.oup.com/edited-volume/41989/chapter/355439648>
- Ding, Jeffrey, and Allan Dafoe. 2021. "The Logic of Strategic Assets: From Oil to AI." *Security Studies* 30 (2): 182–212.
- Dorwart, Hunter, et al. October 19, 2022. "Indonesia's Personal Data Protection Bill: Overview, Key Takeaways, and Context." *Future of Privacy Forum*. <https://fpf.org/blog/indonesias-personal-data-protection-bill-overview-key-takeaways-and-context/>.
- Drezner, Daniel. 2008. *All Politics Is Global: Explaining International Regulatory Regimes*. Princeton, NJ: Princeton University Press.
- Dung, Thuy. August 22, 2022. *Gov't Issues New National Cybersecurity Strategy*. <https://en.baochinhphu.vn/govt-issues-national-strategy-to-combat-new-cyber-security-challenges-111220811103436282.htm>.
- e-Commerce Association of Indonesia. January 14, 2016. "Government Finally Agrees Roadmap Roadmap E-commerce Become a National Program." *idEA*. <https://idea.or.id/artikel/pemerintah-akhirnya-sepakati-petajalan-peta-jalan-e-commerce-menjadi-program-nasional?lang=undefined>.
- Efrat, Asif, and Abraham Newman. 2018. "Divulging Data: Domestic Determinants of International Information Sharing." *The Review of International Organizations* 13: 395–419.
- Ferracane, Martina. 2017. "Restrictions on Cross-Border Data Flows: A Taxonomy." *ECIPE Working Paper* 1.
- Fukuyama, Francis, Barak Richman, and Ashish Goel. 2021. "How to Save Democracy from Technology: Ending Big Tech's Information Monopoly." *Foreign Affairs* 100: 98–110.
- GLobalStats. February, 2023. "Social Media Stats Indonesia." *statcounter*. <https://gs.statcounter.com/social-media-stats/all/indonesia/#yearly-2009-2023>.
- Goddard, Stacie E., Paul K. MacDonald, and Daniel H. Nexon. 2019. "Repertoires of Statecraft: Instruments and Logics of Power Politics." *International Relations* 33 (2): 304–321.
- Goldfarb, Avi, and Jon R. Lindsay. 2021. "Prediction and Judgment: Why Artificial Intelligence Increases the Importance of Humans in War." *International Security* 46 (3): 7–50.
- González, Javier López, Francesca Casalini, and Juan Porras. 2022. "A Preliminary Mapping of Data Localisation Measures." *OECD Trade Policy Paper* 262.
- Government, Indonesian. October 12, 2012. "Number 82 of 2012 Regarding Concerning Electronic System and Transaction Operation." http://www.flevin.com/id/igso/translations/JICA%20Mirror/english/4902_PP_82_2012_e.html.
- Gowa, Joanne, and Edward D. Mansfield. 1993. "Power Politics and International Trade." *American Political Science Review* 87 (2): 408–420.
- Gregory, Robert Wayne, et al. 2021. "The Role of Artificial Intelligence and Data Network Effects for Creating User Value." *Academy of Management Review* 46 (3): 534–551.
- Grossman, Derek, and Christopher Sharman. December 31, 2019. "How to Read Vietnam's Latest Defense White Paper: A Message to Great Powers." *War on the Rocks*. <https://warontherocks.com/2019/12/how-to-read-vietnams-latest-defense-white-paper-a-message-to-great-powers/>.
- Guliani, Akhil, and Michael M. Swift. 2019. "Per-Application Power Delivery." *EuroSys '19: Proceedings of the Fourteenth EuroSys Conference 2019*, Article No: 5, pp. 1–16.
- Heginbotham, Eric, and Richard J. Samuels. 1998. "Mercantile Realism and Japanese Foreign Policy." *International Security* 22 (4): 171–203.
- Hiep, Le Hong. 2019. "The Political Economy of Social Media in Vietnam." *Perspective* 77: 1–7.
- Hirschman, Albert O. 1980. *National Power and the Structure of Foreign Trade*. Berkeley and Los Angeles: University of California Press.

- Hootsuite. February 14, 2022. "5 Major Shifts as Singapore Leaps into a Digital-First World." *Hootsuite*. <https://wearesocial.com.sg/blog/2022/02/5-major-shifts-as-singapore-leaps-into-a-digital-first-world/>.
- Huynh, Triet. September 20, 2021. "Vietnam Digital Economy and Regulatory Challenges." *International Trade Administration*. <https://www.trade.gov/market-intelligence/vietnam-digital-economy-and-regulatory-challenges>.
- Infocomm Media Development Authority. 2017. *Digital Economy Framework for Action*. Singapore: Infocomm Media Development Authority.
- International Telecommunication Union. n.d. "ICT Regulatory Tracker." (). <https://app.gen5.digital/tracker/about>.
- Intersoft Consulting. 2020. *Rights of the Data Subject*. <https://gdpr-info.eu/chapter-3/>.
- Iswaran, S. November 2, 2020. "Closing Speech by Mr S Iswaran, Minister for Communications and Information, at the Second Reading of the Personal Data Protection (Amendment) Bill 2020." *Ministry of Communications and Information*. [https://www.mci.gov.sg/pressroom/news-and-stories/pressroom/2020/11/closing-speech-by-minister-iswaran-at-the-second-reading-of-the-pdp-\(amendment\)-bill-2020](https://www.mci.gov.sg/pressroom/news-and-stories/pressroom/2020/11/closing-speech-by-minister-iswaran-at-the-second-reading-of-the-pdp-(amendment)-bill-2020).
- Jones, Sidney. 2015. "Yudhoyono's Legacy on Internal Security: Achievements and Missed Opportunities." In: *The Yudhoyono Presidency: Indonesia's Decade of Stability and Stagnation*. Edited by Edward Aspinall, Marcus Mietzner, and Dirk Tomsa. Singapore: Institute of Southeast Asian Studies Singapore, pp. 136–154.
- Kennedy, Andrew B., and Darren J. Lim. 2018. "The Innovation Imperative: Technology and US–China Rivalry in the Twenty-First Century." *International Affairs* 94 (3): 553–572.
- Kenney, Martin, and John Zysman. 2016. "The Rise of the Platform Economy." *Issues in Science and Technology* 32 (3): 61–69.
- Keohane, Robert, and Joseph Nye. 2012. *Power and Interdependence: Fourth Edition*. New York: Longman.
- Kissinger, Henry A., Eric Schmidt, and Daniel Huttenlocher. 2021. *The Age of AI and Our Human Future*. New York: Little, Brown, and Company.
- Lau, Lawrence J. 2023. "The Benefits and Potential Costs of a Digital Economy." *Telecommunications Policy* 47 (8): 102594.
- Lawder, David. October 25, 2023. "US Drops Digital Trade Demands at WTO to Allow Room for Stronger Tech Regulation." *Reuters*. <https://www.reuters.com/world/us/us-drops-digital-trade-demands-wto-allow-room-stronger-tech-regulation-2023-10-25/>.
- Levine, Dan. 2018. *Google Data Centers: Economic Impact and Community Benefit*. New York: Oxford Economics.
- Levy, Jack S. 2008. "Case Studies: Types, Designs, and Logics of Inference." *Conflict Management and Peace Science* 25 (1): 1–18.
- Liebowitz, Stan J., and Stephen E. Margolis. 1994. "Network Externality: An Uncommon Tragedy." *Journal of Economic Perspectives* 8 (2): 135–150.
- Liu, Chiu-Wan. 2023. "Conceptualising Private Fintech Platforms as Financial Statecraft and Recentralisation in China." *New Political Economy* 28 (3): 433–451.
- Liu, Lizhi. 2021. "The Rise of Data Politics: Digital China and the World." *Studies in Comparative International Development* 56 (1): 45–67.
- Livia K., and Fadhli Ruhman. August 17, 2022. "Minister Calls for Protection of Indonesia's Digital Sovereignty." *Antara News*. <https://en.antaranews.com/news/244969/minister-calls-for-protection-of-indonesias-digital-sovereignty>.
- Lorentzen, Peter, M. Taylor Fravel, and Jack Paine. 2017. "Qualitative Investigation of Theoretical Models: The Value of Process Tracing." *Journal of Theoretical Politics* 29 (3): 467–491.
- Luong, Dien Nguyen An. 2022. "How the Party-State Retains Controls over Vietnam's Blossoming Media Landscape." *Perspective* 79.
- MacKinnon, Rebecca. 2011. "Liberation Technology: China's Networked Authoritarianism." *Journal of Democracy* 22 (2): 32–46.
- Mahoney, James. 2007. "Qualitative Methodology and Comparative Politics." *Comparative Political Studies* 40 (2): 122–144.
- Mai, Ngoc. September 8, 2018. "Vietnam Minister Wants Local Social Networks to Compete with Facebook, Google." *Hanoi Times*. <https://hanoitimes.vn/vietnam-minister-wants-local-social-networks-to-compete-with-facebook-google-3075.html>.
- Martens, Bertin. 2021. "An Economic Perspective on Data and Platform Market Power." *JRC Digital Economy Working Paper* 2020-09, pp. 54–59.
- Massmann, Oliver. June 7, 2023. "Vietnam – Latest draft of the Cybersecurity Administrative Sanctions Decree – What You Must Know." *Duane Morris LLP*. <https://blogs.duanemorris.com/vietnam/2023/06/07/vietnam-latest-draft-of-the-cybersecurity-administrative-sanctions-decree-what-you-must-know/>.
- Mastanduno, Michael. 1991. "Do Relative Gains Matter?: America's Response to Japanese Industrial Policy." *International Security* 16 (1): 73–113.
- Mastanduno, Michael. 1998. "Economics and Security in Statecraft and Scholarship." *International Organization* 52 (4): 825–854.
- Mawangi, Genta Tenri, and T. Kenzu. July 22, 2021. "Telkom Urged to Reinforce Indonesia's Data Sovereignty: Legislator." *Antara News*. <https://en.antaranews.com/news/180170/telkom-urged-to-reinforce-indonesias-data-sovereignty-legislator>.
- Mazurek, Grzegorz, and Karolina Malagocka. 2019. "Perception of Privacy and Data Protection in the Context of the Development of Artificial Intelligence." *Journal of Management Analytics* 6 (4): 344–364.
- McKnight, Scott, Martin Kenney, and Dan Breznitz. 2023. "Regulating the Platform Giants: Building and Governing China's Online Economy." *Policy & Internet* 15 (2): 153–282.
- Meltzer, Joshua. 2020. "The Digital Transformation of International Trade." In: *Growth in a Time of Change: Global and Country Perspectives on a New Agenda*. Edited by Hyeon-Wook Kim, and Zia Qureshi. Washington, DC.: Brookings Institution Press, pp. 173–208.

- Ministry of Communication and Informatics. December 18, 2011. "Data Center Development Rules Still Harmonized (Aturan Pembangunan Data Center Masih Diharmonisasi)." *Ministry of Communication and Informatics*. <https://www.kominfo.go.id/content/detail/1673/aturan-pembangunan-data-center-masih-diharmonisasi/0/sorotanmedia>.
- Ministry of Communication and Informatics. March 22, 2022. "Fighting For Digital Sovereignty, MOCI: Indonesia Stretches Four Main Principles Of Cross-Border Data Flow (Perjuangkan Kedaulatan Digital, Menkominfo: Indonesia Usung Empat Prinsip Utama Arus Data Lintas Batas Negara)." *Press Release*. 98/HM/KOMINFO/03/2022. <https://www.kominfo.go.id/content/detail/40711/siaran-pers-no-98hmkominfo032022-tentang-perjuangkan-kedaulatan-digital-menkominfo-indonesia-usung-empat-prinsip-utama-arus-data-lintas-batas-negara/0/siaranpers>.
- Ministry of Communication and Informatics. September 20, 2022. "Guarantee Citizens' Rights, Minister Johnny: Indonesia Becomes the Fifth Country in ASEAN to Have Personal Data Rules (Jamin Hak Warga Negara, Menteri Johnny: Indonesia Jadi Negara Kelima di ASEAN Miliki Aturan Data Pribadi)." *Ministry of Communication And Informatics*. https://www.kominfo.go.id/content/detail/44424/siaran-pers-no-419hmkominfo092022-tentang-jamin-hak-warga-negara-menteri-johnny-indonesia-jadi-negara-kelima-di-asean-miliki-aturan-data-pribadi/0/siaran_pers.
- Ministry of Communication and Informatics. July 23, 2020. "Indonesia Calls for Data Sovereignty and Security at G20 Digital Economy Ministerial Meeting (Indonesia Serukan Kedaulatan dan Keamanan Data dalam G20 Digital Economy Ministerial Meeting)." *Diskominfortik*. <https://diskominfo.bandacehkota.go.id/2020/07/23/indonesia-serukan-kedaulatan-dan-keamanan-data-dalam-g20-digital-economy-ministerial-meeting/>.
- Ministry of Communication and Informatics. August 17, 2022. "Moment of the 77th Anniversary of Indonesian Independence, MOCI Emphasizes Digital Sovereignty (Momen HUT ke-77 Kemerdekaan RI, Menkominfo Tekankan Kedaulatan Digital)." *Press Release* 329/HM/KOMINFO/08/2022. https://www.kominfo.go.id/content/detail/43745/siaran-pers-no-329hmkominfo082022-tentang-momen-hut-ke-77-kemerdekaan-ri-menkominfo-tekanan-kedaulatan-digital/0/siaran_pers.
- Ministry of Communication and Informatics. December 1, 2016. "Number 20 of 2016 Regarding Protection of Personal Data in Electronic System." *maka*. <http://makna.co/wp-content/uploads/2018/01/MOCI-Regulation-No-20-of-2016-Makna-Eng.pdf>.
- Ministry of Communication and Informatics. March 11, 2019. "RIF 2019 Offers Digital Economy and Tourism Investment Opportunities (RIF 2019 Tawarkan Peluang Investasi Ekonomi Digital dan Pariwisata)." *Ministry of Communication and Informatics*. <https://www.kominfo.go.id/index.php/content/detail/17032/rif-2019-tawarkan-peluang-investasi-ekonomi-digital-dan-pariwisata/0/artikelgpr>.
- Ministry of Communication and Informatics. March 15, 2016. "The Potential of the Digital Economy Must Be Exploited (Potensi Ekonomi Digital Harus Dimanfaatkan)." *Ministry of Communication and Informatics*. https://www.kominfo.go.id/content/detail/7097/potensi-ekonomi-digital-harus-dimanfaatkan/0/sorotan_media.
- Ministry of Communications and Information. June 27, 2023. "New UK- Singapore Agreements on Data and Emerging Technologies to Help Boost Trade and Security." *Ministry of Communications and Information*. <https://www.mci.gov.sg/pressroom/news-and-stories/pressroom/2023/6/new-uk-singapore-agreements-on-data-and-emerging-technologies-to-help-boost-trade-and-security>.
- Ministry of Defence. 2008. *Defence White Paper 2008*. Jakarta: Ministry of Defence.
- Ministry of Defence. 2015. *Defence White Paper 2015*. Jakarta: Ministry of Defence.
- Ministry of Industry. 2018. "Making Indonesia 4.0." *Ministry of Industry*. https://sea-vet.net/images/seb/initiatives/appendix_file/570/making-indonesia-40-bppi.pdf.
- Ministry of Information and Communications. November 17, 2021. "Data Defined as New Resource for Economic and Social Development." *Vietnam Ministry of Information and Communications*. <https://english.mic.gov.vn/Pages/TinTuc/150323/Data-defined-as-new-resource-for-economic-and-social-development.html>.
- Ministry of Information and Communications. December 26, 2016. "Detailing Cross-Border Provision of Public Information." *Centre Database on Legal Normative Documents*. <https://vbpl.vn/tw/Pages/vbpqen-toanvan.aspx?ItemID=11120>.
- Ministry of Law and Human Rights. April 21, 2008. "Law of the Republic of Indonesia Number 11 of 2008." *President of the Republic of the Indonesia*. https://www.icnl.org/wp-content/uploads/Indonesia_elec.pdf.
- Ministry of Law and Human Rights. August 3, 2017. *Road Map E-Commerce (Peta Jalan Sistem Perdagangan Nasional Berbasis Elektronik)*. Jakarta: President of the Republic of the Indonesia.
- Ministry of Trade. 2021. *Information on International Trade Negotiations Communication Services Sector in Indonesia (Informasi Perundingan Perdagangan Internasional Sektor Jasa Komunikasi di Indonesia)*. Jakarta: Ministry of Trade.
- Ministry of Trade and Industry. 2023a. *Digital Economy Agreements*. <https://www.mti.gov.sg/Trade/Digital-Economy-Agreements>.
- Ministry of Trade and Industry. February 2023b. *European Union – Singapore Digital Partnership*. <https://www.mti.gov.sg/Trade/Digital-Economy-Agreements/EUSDP>.
- Mueller, Milton L. 2020. "Against Sovereignty in Cyberspace." *International Studies Review* 22 (4): 779–801.
- Mulyanto, Randy, and Leo Galuh. August 4, 2022. "Indonesia's PayPal, Yahoo Bans Cast Cloud Over Tech Hub Dream." *Aljazeera*. <https://www.aljazeera.com/economy/2022/8/4/indonesias-paypal-ban-casts-cloud-over-tech-hub-dreams>.
- Na, Xuanming, and Yulong Ma. 2021. "Analysis of Monopoly in Platform Economy and Suggestions for Countermeasures." *International Conference on Society Science 2021*: 329–332.
- National Academy of Public Administration. March 31, 2022. "National Strategy for Development of Digital Economy and Digital Society to 2025, Orientation to 2030." *National Academy of Public Administration*. <https://www1.napa.vn/en/national-strategy-for-development-of-digital-economy-and-digital-society-to-2025-orientation-to-2030.napa>.

- Natisha, A., and Fadhli Ruhman. June 18, 2022. "Minister Outlines Importance of Discussing Cross-Border Data Flow." *Antara News*. <https://en.antaranews.com/news/234921/minister-outlines-importance-of-discussing-cross-border-data-flow>.
- Newman, Abraham. 2008. *Protectors of Privacy: Regulating Personal Data in the Global Economy*. Ithaca: Cornell University Press.
- Newman, Abraham, and Elliot Posner. 2011. "International Interdependence and Regulatory Power: Authority, Mobility, and Markets." *European Journal of International Relations* 17 (4): 589–610.
- Nguyen, Phuong. August 18, 2021. "Vietnam Orders Tech Firms to Store User Data Onshore." *Reuters*. <https://www.reuters.com/world/asia-pacific/vietnam-orders-tech-firms-store-user-data-onshore-2022-08-18/>.
- Norris, William J. 2016. *Chinese Economic Statecraft: Commercial Actors, Grand Strategy, and State Control*. Ithaca: Cornell University Press.
- O'Leary, Daniel E. 2013. "Artificial Intelligence and Big Data." *IEEE Intelligent Systems* 28 (2): 96–99.
- O'Connor, Brendan. 2015. "Quantifying the Cost of Forced Localization." *Leviathan Security Group*. <https://static1.squarespace.com/static/6128b1eb2eb2cf15b7a35a2f/t/65af6b484ec970386fd56386/1705995081389/Quantifying%2Bthe%2BCost%2Bof%2BForced%2BLocalization.pdf>
- Obendiek, Anke Sophia. 2022. "What Are We Actually Talking About? Conceptualizing Data as a Governable Object in Overlapping Jurisdictions." *International Studies Quarterly* 66 (1): sqab080. <https://doi.org/10.1093/isq/sqab080>.
- OECD. December 11, 2011. "OECD Council Recommendation on Principles for Internet Policy Making." *OECD*. <https://www.oecd.org/sti/ieconomy/49258588.pdf>.
- Pamuk, Humeyra, and Stanley Widiyanto. December 13, 2021. "Indonesia Cites Strong U.S. Commitment as Blinken Starts Southeast Asia Tour." *Reuters*. <https://www.reuters.com/world/asia-pacific/blinken-indonesia-us-seeks-shore-up-southeast-asia-ties-2021-12-13/>.
- Pang, Eul-Soo. 2011. *The US-Singapore Free Trade Agreement: An American Perspective on Power, Trade, and Security in the Asia Pacific*. Singapore: Institute of Southeast Asian Studies.
- Parekh, Satyajit, et al. June 20, 2022. "Localization of Data Privacy Regulations Creates Competitive Opportunities." *McKinsey & Company*. <https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/localization-of-data-privacy-regulations-creates-competitive-opportunities/>.
- Pearson, James, and Khanh Vu. November 8, 2018. "Vietnam Wants 50 Percent of Social Media Users on Domestic Platforms by 2020." *Reuters*. <https://www.reuters.com/article/ctech-us-vietnam-socialmedia-idCAKCNIND1FM-OCATC>.
- Personal Data Protection Commission. 2022. *Advisory Guidelines on Key Concepts in the Personal Data Protection Act*. Singapore: Personal Data Protection Commission.
- Pham, Nam. 2017. "Data Centers: Jobs and Opportunities in Communities Nationwide." *US Chamber of Commerce Technology Engagement Center*. <https://www.uschamber.com/technology/data-centers-jobs-opportunities-communities-nationwide>.
- Plate, Johnny. 2022. *G20 Digital Economy Ministers' Meeting 2022 Chair's Summary*. Jakarta: G20 Indonesia 2022.
- Potkin, Fanny, and Phuong Nguyen. September 28, 2022. "Vietnam Preparing Rules to Limit News Posts on Social Media Accounts-Sources." *Reuters*. <https://www.reuters.com/technology/exclusive-vietnam-preparing-rules-limit-news-posts-social-media-accounts-sources-2022-09-28/>.
- Potluri, Sai Rakshith, V. Sridhar, and Shrishra Rao. 2020. "Effects of Data Localization on Digital Trade: An Agent-Based Modeling Approach." *Telecommunications Policy* 44 (9): 102022.
- Powers, Shawn M., and Michael Jablonski. 2015. *The Real Cyber War: The Political Economy of Internet Freedom*. Urbana: University of Illinois Press.
- Presidential Staff Office. March 9, 2023. "Coordinating Minister for Air- langga: Optimism for Good Economic Performance Needs to be Supported by Great Potential in the Digital Sector (Menko Airlangga: Optimisme Kinerja Ekonomi yang Baik Perlu Didukung oleh Potensi Besar di Sektor Digital)." *Press Release HM.4.6/87/SET.M.EKON.3/03/2023*. <https://www.ekon.go.id/publikasi/detail/5003/menko-airlangga-optimisme-kinerja-ekonomi-yang-baik-perlu-didukung-oleh-potensi-besar-di-sektor-digital>.
- Presidential Staff Office. October 26, 2022. "Moeldoko: Indonesia Is Serious About Realizing Digital Sovereignty (Moeldoko: Indonesia Serius Mewujudkan Kedaulatan Digital)." *News*. <https://www.ksp.go.id/moeldoko-indonesia-serius-mewujudkan-ke-aulatan-digital.html>.
- Priyandita, Gatra, Dirk van der Kley, and Benjamin Herscovitch. 2022. "Localization and China's Tech Success in Indonesia." *Carnegie Endowment for International Peace*. https://carnegieendowment.org/files/van_der_Kley_et_al_China_Indonesia_fina11.pdf.
- Putri, Lifa, and Fadhli Ruhman. March 23, 2022. "Minister Outlines Priorities Within Digital Indonesia Road Map." *Antara*. <https://en.antaranews.com/news/221329/minister-outlines-priorities-within-digital-indonesia-road-map>.
- PwC. November, 2019. "Digital Trust Newsflash." *PwC 1*. <https://www.pwc.com/id/en/services/assets/risk-assurance/newsflash/ra-newsflash-2019-01.pdf>.
- Reisman, Dillon. May 22, 2017. "Where Is Your Data, Really?: The Technical Case Against Data Localization." *Lawfare*. <https://www.lawfareblog.com/where-your-data-really-technical-case-against-data-localization>.
- Richardson, J. David. 1990. "The Political Economy of Strategic Trade Policy." *International Organization* 44 (1): 107–135.
- Rod, Espen Geelmuyden, and Nils B. Weidmann. 2015. "Empowering Activists or Autocrats? The Internet in Authoritarian Regimes." *Journal of Peace Research* 52 (3): 338–351.
- Ryan, Patrick S., Sarah Falvey, and Ronak Merchant. 2013. "When the Cloud Goes Local: The Global Problem with Data Localization." *Computer* 46 (1): 54–59.

- Sargsyan, Tatevik. 2016. "Data Localization and the Role of Infrastructure for Surveillance, Privacy, and Security." *International Journal of Communication* 10: 17.
- Seawright, Jason, and John Gerring. 2008. "Case Selection Techniques in Case Study Research: A Menu of Qualitative and Quantitative Options." *Political Research Quarterly* 61 (2): 294–308.
- Singapore Government. December 21, 2022. "Personal Data Protection Act 2012." *Singapore Statutes Online*. <https://sso.agc.gov.sg/Act/PDPA2012?ProvIds=P13-#P13->.
- Slaughter Matthew, J., and David H. McCormick. 2021. "Data Is Power: Washington Needs to Craft New Rules for the Digital Age." *Foreign Affairs* 100 (3): 54–62.
- Suneja, Kirtika. May 4, 2018. "US, Japan and Singapore Propose Free Flow of Data, Oppose Server Localisation." *The Economic Times*. <https://economictimes.indiatimes.com/news/economy/policy/us-japan-singapore-propose-free-flow-of-data-oppose-server-localisation/articleshow/64020980.cms?from=mdr>.
- Swire, Peter, and DeBrae Kennedy-Mayo. 2022. "The Effects of Data Localization on Cybersecurity." *Georgia Tech Scheller College of Business Research Paper* 4030905.
- Technology Assessment and Assessment Agency (BPPT). 2020. *Indonesian National Strategy for AI 2020-2045 (Strategi Nasional Kecerdasan Artifisial Indonesia)*. Jakarta: BPPT.
- Teo, Josephine. March 4, 2022. "Committee of Supply – Head Q (Ministry of Communications and Information)." *Singapore Parliament*. <https://sprs.parl.gov.sg/search/#/sprs3topic?reportid=budget-1862>.
- Teo, Josephine. December 1, 2022. "Speech by Mrs Josephine Teo, Minister of Communications and Information, at the Global Technology Summit." *Ministry of Communications and Information*. <https://www.mci.gov.sg/pressroom/news-and-stories/pressroom/2022/12/speech-by-minister-of-communications-and-information-josephine-teo-at-the-global-technology-summit-on-1-december-2022>.
- Teo, Josephine. April 5, 2023. "Transcript of Comments Made by Mrs Josephine Teo, Minister for Communications and Information." *Ministry of Communications and Information*. <https://www.mci.gov.sg/pressroom/news-and-stories/pressroom/2023/4/transcript-of-comments-made-by-minister-josephine-teo-at-panel-session-on-cyber-strategy-and-digital-governance-protecting-sovereignty-and-building-resilience-of-the-sydney-dialogue>.
- Thelen, Kathleen. 2018. "Regulating Uber: The politics of the platform economy in Europe and the United States." *Perspectives on Politics* 16 (4): 938–953.
- Trampusch, Christine, and Bruno Palier. 2016. "Between X and Y: How Process Tracing Contributes to Opening the Black Box of Causality." *New Political Economy* 21 (5): 437–454.
- Tu, Dang Cam, and Hang Thi Thuy Nguyen. 2019. "Understanding the US–Vietnam Security Relationship, 2011–2017." *The Korean Journal of Defense Analysis* 31 (1): 121–144.
- Tusikov, Natasha. 2017. *Chokepoints: Global Private Regulation on the Internet*. Oakland: University of California Press.
- Tusikov, Natasha. 2021. "Internet Platforms Weaponizing Choke Points." In: *The Uses and Abuses of Weaponized Interdependence*. Edited by Daniel Drezner, Henry Farrell, and Abraham Newman. Washington, DC: Brookings Institution Press, pp. 133–148.
- Tyson, Laura, and John Zysman. 1983. "American Industry in International Competition: Government Policies and Corporate Strategies." *California Management Review* 25 (3): 27–52.
- US Department of Commerce. April 22, 2022. "Global Cross-Border Privacy Rules Declaration." *US Department of Commerce*. <https://www.commerce.gov/global-cross-border-privacy-rules-declaration>.
- US Department of Commerce. October 27, 2022. "Joint Statement: U.S. Department of Commerce and Singapore Ministry of Trade and Industry Celebrate Inaugural U.S.-Singapore Partnership for Growth and Innovation Annual Dialogue." *US Department of Commerce*. <https://www.commerce.gov/news/press-releases/2022/10/joint-statement-us-department-commerce-and-singapore-ministry-trade-and>.
- US Department of Defense. 2020. *DoD Data Strategy*. Washington, DC: Department of Defense.
- US Department of Treasury. February 5, 2020. "United States – Singapore Joint Statement on Financial Services Data Connectivity." *US Department of Treasury*. <https://home.treasury.gov/news/press-releases/sm899>.
- US International Trade Commission. 2014. *Digital Trade in the U.S. and Global Economies, Part 2*. Washington, DC: US International Trade Commission.
- US Trade Representative. 2023. *2023 National Trade Estimate Report on Foreign Trade Barriers*. Washington, DC: Office of the United States Trade Representative.
- US Trade Representative. April 2013. "2014 Section 1377 Review." *Office of the US Trade Representative*. <https://ustr.gov/sites/default/files/2013-14%5C%20-1377Report-final.pdf>.
- US Trade Representative. March 2017. "Key Barriers to Digital Trade." *Office of the US Trade Representative*. <https://ustr.gov/about-us/policy-offices/press-office/fact-sheets/2017/march/key-barriers-digital-trade>.
- Van Puyvelde, Damien, Stephen Coulthart, and M Shahriar Hossain. 2017. "Beyond the Buzzword: Big Data and National Security Decision-Making." *International Affairs* 93 (6): 1397–1416.
- VanLear, Sara, et al. 2020. "The Impact of Facebook's U.S. Data Center Fleet." *RTI International*. <https://www.rti.org/publication/impact-facebooks-us-data-center-fleet-2017-2019/fulltext.pdf>.
- Vietnam Government. April 23, 2023. "Decree On Personal Data Protection." *European Chamber of Commerce in Vietnam*. <https://eurochamvn.org/wp-content/uploads/2023/02/Decree-13-2023-PDPDENclean.pdf>.
- Vy, Tran Si. October, 2022. "Issue of October 2022." *ENT Law LLC*. <https://entlaw.com.vn/data-storage-decree-53/>.
- Waldner, David. 2015. "Process Tracing and Qualitative Causal Inference." *Security Studies* 24 (2): 239–250.

- Widianto, Stanley. September 20, 2022. "Indonesia Parliament Passes Long-awaited Data Protection Bill." *Reuters*. <https://www.reuters.com/world/asia-pacific/indonesia-parliament-passes-long-awaited-data-protection-bill-2022-09-20/>.
- World Bank. 2021. *Shifting Gears: Digitization and Services-Led Development*. Washington, DC: The World Bank.
- Wu, Emily. July, 2021. "Sovereignty and Data Localization." *The Cyber Project Report*: 18. <https://www.belfercenter.org/sites/default/files/2021-07/SovereigntyLocalization.pdf>.
- Zhang, Qianwen, and Andrew Mitchell. 2022. "Data Localization and the National Treatment Obligation in International Investment Treaties." *World Trade Review* 21 (4): 391–410.
- Zhu, Feng, and Marco Iansiti. 2019. "Why Some Platforms Thrive and Others Don't." *Harvard Business Review*. <https://hbr.org/2019/01/why-some-platforms-thrive-and-others-dont>.
- Zuboff, Shoshana. 2019. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: Profile books.