Does **Data Localization** Adequately Balance **Privacy and Security?**

Columbia SIPA Capstone Report
May 2023

Does Data Localization Adequately Balance Privacy and Security?

Faculty Adviser: Adam Segal

Authors: Betül Demirel, Jiaxun (Leila) Li,
Venesa Rugova, Tsubasa Watanabe, Daisy Zhao

Columbia University
School of International and Public Affairs (SIPA)

Capstone Report

Published in May 2023

Design by Jiaxun (Leila) Li, Tsubasa Watanabe ©

Cover page image from Canva
Page 4, 8, 12, 28 images from Unsplash
Page 6 image from Pexels
Page 23 image from Shutterstock
Page 25 image from Palo Alto Networks, Unit 42

Acknowledgment

The Columbia SIPA Capstone team would like to extend our gratitude to our mentors, interviewees, participants, and advisors who made our research possible and creative.

We would first like to thank all the experts and professionals who took the time to share their perspectives and experiences, in particular: Arun Warikoo (BNP Paribas), William Drake (Columbia Business School), Daniel Dobrygowski (World Economic Forum), Trip Boyer (Palo Alto Networks), Pam Kingpetcharat (Columbia University), Lily Fang (Palo Alto Networks), Neal Pollard (Ernst & Young), Jen Miller-Osborn (Palo Alto Networks), Jason Harrell (The Depository Trust & Clearing Corporation), Nigel Cory (Information Technology and Innovation Foundation). Their participation in our research has furthered our understanding of the challenges caused by data localization around the world and the possible future regulatory frameworks. The candid responses of the interviewees directly informed our recommendations to promote an ecosystem that better accounts for cybersecurity interests.

At SIPA, we are particularly grateful to Professor Adam Segal, Adjunct Professor of International and Public Affairs, whose advice and feedback guided us throughout this research project. We are also grateful to Saleha Awal, Suzanne Hollmann, and the rest of the Columbia SIPA Capstone Program for their logistical support. In addition, we appreciate the feedback of SIPA faculty members Daniel Dobrygowski, Elana Broitman, and Munish Walther-Puri, who offered helpful input to our research plan.

Finally, we would like to thank our client Palo Alto Networks. We are especially grateful to Sam Kaplan, Senior Policy Counsel at Palo Alto Networks, who provided us with a wealth of information, engagement with the project, and valuable contacts to better understand the difficulties facing the cybersecurity ecosystem.

The findings and recommendations contained herein reflect the opinion and conclusions of the research team and not the position or opinion of Palo Alto Networks, Inc. or its affiliates.

Contents

Executive Summary

This paper joins the evolving discussion on the unintended consequences of data localization policies on defensive cybersecurity, another legitimate public policy objective. This paper encourages cybersecurity policy professionals to highlight this ecosystem problem more and set up a process to address these concerns collectively.

Part I How Data Localization Affects Cybersecurity

The first part of the paper examines how existing data localization policies primarily motivated by privacy and data protection reasons affect cyber threat information sharing, including:

(1) Identified legislative trends in data localization policies in 12 representative countries and the European Union before April 2023;

(2) Analyzed data localization effects on cybersecurity, particularly cyber threat information sharing from a literature review, interviews with 16 policy and industry experts, and two case studies.

Key Findings:

- The legislation review of the selected sample finds no national policies that explicitly account for the sharing of cyber threat information and adequately balance the need to protect or localize such data and need for cyber threat information sharing.
  - A significant number of new proposals among the surveyed policies (27% of the sampled policies) suggests that data localization policies are still on the rise;
  - The common trend is that sector-specific data localization policies (64% of the sampled policies) target four sectors: Financial Services, ICT, Public Sector, and Healthcare.
- The literature review and interviews showed that data localization does have a negative impact on cybersecurity. However, the lack of consensus on the scope of data localization

and the measurement of domestic cyber resilience makes it challenging to specify the costs.

- One of the direct costs is reflected in cross-border cyber threat information sharing where:
  - Restrictions on a broad set of data debilitate the cyber threat intelligence process for both integrated cybersecurity management and third-party cybersecurity services;
  - The inability to aggregate data at scale limits the development of advanced analytics tools using AI/ML technologies.
- This paper found no distinct event or incident where data localization policies undermined cyber defenses, but two case studies show potential harms:
  - **Cloudflare for 2021 Portugal Census:**
    This broad enforcement of GDPR caused a European public entity to lose real-time cyber threat monitoring services;
  - **Palo Alto Networks Unit 42 Detection of Chinese APT "GALLIUM":**
    Data localization would debilitate the cyber threat intelligence process that successfully detected GALLIUM infrastructure and targeted entities across nine countries.

Part II Alternative Regulatory Frameworks

The second part of the paper examines five regulatory approaches to cross-border data flows, evaluating them on five criteria: interoperability, timeliness, persistency, transparency, and enforcement.

Key Recommendations:

- Recommended Regulatory Framework:
  - The "accountability-based" approach, exemplified by the APEC Cross-Border Privacy Rules (CBPR) System, is a pragmatic regulatory framework that balances privacy and security interests, especially cross-border cyber threat information sharing.
- Recommendations for Policy Engagement and Research:
  - Highlight cybersecurity policy objectives hindered by data localization by participating in multistakeholder forums through tech trade associations and investing in cybersecurity coalitions;
  - Encourage internal and industry-wide publication of case studies highlighting how data localization harms critical cross-border threat information sharing;
  - Future research topics include mapping the stakeholders, aggregating industry comments to policy proposals, and developing metrics to quantify the impact on cyber resilience.

1. Introduction

With the topic of this report coming from Palo Alto Networks, a global cybersecurity company headquartered in California, the Columbia University School of International and Public Affairs (SIPA) capstone team has conducted a comprehensive analytical project to assess the effect of data localization policies on domestic cyber resilience and explore regulatory frameworks that better balance privacy and cybersecurity.

In completing this project, the Capstone team worked closely with the Office of Cybersecurity Strategy and Global Policy, whose objective is to contribute to the core mission of Palo Alto Networks — protecting our digital way of life, by providing analyses of global government legislation, policies, regulations, and programs affecting companies in this field.

The first part of the paper examines whether existing data localization policies designed to address privacy interests effectively enhance domestic cyber resilience. The team conducted a survey of existing and proposed legislation, highlighting trends in the selected countries and regions. It also reviewed the existing research and conducted interviews with practitioners active at the intersection of data localization and cybersecurity. Two real-world case studies help illustrate some current and potential tensions between data localization and cybersecurity.

The second part of the paper unpacks which particular regulatory frameworks for data localization better account for cybersecurity interests. The paper identifies categorized regulatory frameworks underlying countries' approach to data localization, creates criteria to evaluate these regulatory frameworks, and offers policy recommendations.

2. Background

2.1. Motivations of Data Localization

A growing number of countries have adopted data localization policies, in part, based on the premise that storing data locally improves security and privacy.

Data localization policies in this study refer to national policies that require the processing or storage of data within a country's borders. While there is no single definition of data localization agreed upon by policymakers (López González et al., 2022)**,** data localization ranges from "hard" policies that prohibit the cross-border transfer of the original data to "soft" policies that require a copy of the data to be stored or mirrored in the country (Swire & Kennedy-Mayo, 2022, p.4). This study groups data localization policies into (1) direct and explicit policies that require localization; (2) indirect and de facto policies that have the consequence of localization; (3) and proposed legislation or directives (Cory & Dascoli, 2021).

Countries require data localization out of a mix of four motivations: privacy and data protection, national security, economic interests, and digital sovereignty (López González et al., 2022; Cory & Dascoli, 2021; Swire & Kennedy-Mayo, 2022; Centre for Information Policy Leadership, 2023).

Table 1 Motivations of Data Localization

Motivation	Description
Privacy and Data Protection	Domestic storage of data is perceived to be a means to ensure compliance with domestic privacy and data protection laws, which govern "who should be authorized to access data" (Swire & Kennedy-Mayo, 2022, p. 7).
National Security	Data localization can facilitate government access to data for legitimate purposes, such as law enforcement and regulatory oversight, or more controversial purposes, like censorship and surveillance.
Economic Interest	Imposing barriers to cross-border data flows can be applied with industrial policies to support the development of local cloud, data analytics, or other IT service sectors.
Data Sovereignty	Data sovereignty, also known as digital sovereignty or cyber sovereignty, vaguely refers to the "assertion of state control over data, data flows, and digital technologies" (Cory & Dascoli, 2021, p. 6).

Understanding the mixed motivations behind each national policy of data localization is the first step in identifying the gaps in the regulatory framework. Besides the stated objectives, data localization policies can mask hidden motivations when the policymaking process lacks evidence and transparency (Cory & Dascoli, 2021).

2.2. Motivations of the Study

Economic analysis and real-life examples support the negative impact of data localization on the macroeconomy. Cory and Dascoli (2021) measured the negative impact data localization has on trade, productivity, and costs in affected industries using a scale based on OECD market-regulation data: the study finds that a 1-point increase in a country's data restrictiveness, on average, is associated with a 7-percent decrease in its trade output and a 2.9-percent decrease in its productivity.

On the micro level, data localization has direct business, societal, and consumer impacts. Data localization undermines business functions that require cross-border data transfers, including cybersecurity-related tools and services, human resources systems, fraud prevention services, manufacturing operations, and customer services. These policies impede individuals' access to legitimate-use products and services, including cloud computing services, financial services, cross-border research collaboration, 5G telecommunications infrastructure, social media services and communications, and modern farming technology (Centre for Information Policy Leadership, 2023).

While the economic effects of data localization policies are well documented, their effects on cybersecurity are under-explored. According to Nigel Cory (personal communication, April 11, 2023) of the Information Technology and Innovation Foundation (ITIF), data localization is particularly misguided in the cybersecurity sphere.

This qualitative study employs a mix of literature review, an examination of legislation reviews of data localization policies in 12 representative countries and the European Union (EU), 16 interviews with industry and policy experts, and two case studies. This study focuses on defensive cybersecurity, technologies and processes used to identify, protect, detect, respond and recover from cyber-attacks to ensure the confidentiality, integrity, and availability (known as the CIA triad) of information and information systems (Cawthra et al., 2020).

Security and privacy share a similar goal of "preventing unauthorized access," but Swire and Kennedy-Mayo (2022) argue that data localization may, in fact, force tradeoffs between the two objectives: **"A measure designed to increase privacy reduces cybersecurity to the extent the privacy measure increases the risk of unauthorized access, reduces integrity, or reduces availability"** (p. 7). A data localization policy, even though intended to enhance data security, may lose sight of the de facto effects harming security, such as cutting off cross-border cyber threat detection.

Specifically, data localization reduces cross-border sharing of information, including cyber threat information. According to the U.S. National Institute of Standards and Technology (NIST), **cyber threat information** is "any information that can help an organization identify, assess, monitor, and respond to cyber threats"; **indicators of compromise** include "tactics, techniques, and procedures used by threat actors; suggested actions to detect, contain, or prevent attacks; and the findings from the analyses of incidents" (Johnson et al., 2016, p. ii). Personal and non-personal data both provide useful information for an organization to identify cyber threats. Data localization focused on personal data, therefore, can thwart an organization's cybersecurity management across its global offices or with third-party cybersecurity service providers in another jurisdiction.

In addition, cyber threat detection requires the real-time gathering of information that describes an organization's cybersecurity posture. The local processing or storage of this data may prevent organizations from transferring data in or out of a jurisdiction, limiting their ability to aggregate data and transform it into intelligence in a timely manner.

Furthermore, data localization has a negative effect broadly on cyber resilience. Harmonizing definitions from IBM and NIST, **cyber resilience** (or cyber resiliency) is the ability to anticipate, withstand, recover from, and adapt to cyber-attacks (IBM, n.d.; NIST, n.d., Glossary: "cyber resiliency").

This study contributes to the literature by focusing on the underexplored nexus of data localization and cybersecurity. After examining data localization's effects through the lens of cybersecurity and cyber resilience, this study aims to identify future regulatory frameworks that balance privacy and security interests and serve as pragmatic alternatives to data localization policies of today.

Do data localization policies adequately balance privacy and security interests? This study breaks down the central inquiry into two questions:

- Are existing data localization policies, primarily motivated by privacy and data protection, helpful in enhancing cybersecurity and cyber resilience?
- Are there existing or potential regulatory frameworks that better account for providing and sharing cyber threat information across borders?

3. Data Localization and Cybersecurity

3.1. Legislation Landscape

Samples and Taxonomy of Data Localization Policies

Before investigating the impact of data localization policies on cybersecurity, a preliminary legislative review of current policies was conducted.

This legislation review used a sample of 12 representative countries[1] and the EU (Figure 1), selected based on the following criteria:

- Does Palo Alto Networks have a presence in the country (offices, private partnerships, R&D centers)?
- Does the country have influential data-localization policies or proposals?
- Does the sample cover the major digital economies in every geographical region?

The review was conducted primarily by examining secondary sources, such as academic papers and articles published by prominent law firms, but for some countries, primary sources (original texts of laws and guidelines) were also reviewed.

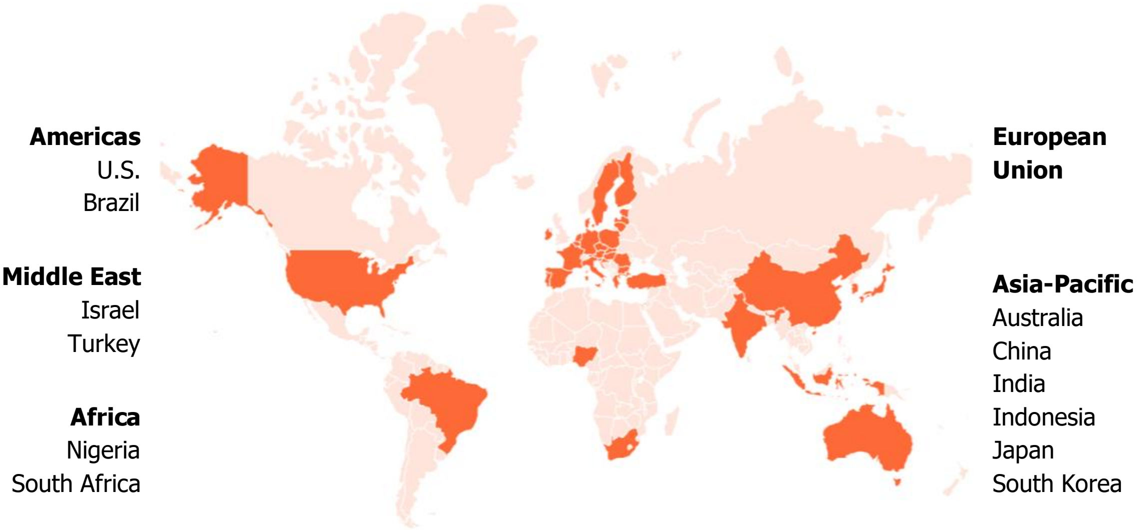


Figure 1 The Selected Jurisdictions for the Legislation Review

[1] The review was also conducted on Singapore's data policies but did not identify any data localization policy, so it does not include Singapore in its samples.

This paper categorizes data localization policies in these jurisdictions in accordance with the following criteria (Cory & Dascoli, 2021):

- **Direct (explicit) policies:** policies require firms to locate or process the original or copy of data in the country by law.
- **Indirect (de facto) policies:** policies make it difficult for firms to locate data in other countries virtually (by any means).
- **Proposals:** a proposed new data localization policy (either direct or indirect).

In addition to this classification, the review used the taxonomy of hard data localization policies that "require that certain data be stored within certain borders and not copied or transmitted anywhere else" and soft data localization policies that "involves 'mirroring,' requiring that copies of a certain kind of data be stored within a certain area but does not restrict the copying or transmission of that data elsewhere" (Daskel & Sherman, 2020, p. 7).

The review identified 67 policies in the sample jurisdictions, which were, in principle, counted by the number of laws (or bills in the case of proposals). However, a single law, bill, or draft policy containing multiple data localization measures of clearly different natures was counted as multiple policies. For example, the Draft National Policy on Data and Cloud, published by the South African government in April 2021, includes several data localization measures with different degrees of stringency against "data classified/identified as critical Information Infrastructure," "data generated from South African natural resources," citizen data" and "research data" (Department of Communications and Digital Technologies of South Africa, 2021, pp. 27-28). Therefore, the review counted this single proposal as four policies.

Findings

There are a significant number of new proposals among the surveyed policies, suggesting that data localization policies are still on the rise. Of the 67 policies identified by this review, one-fourth (18 policies) were proposals. The number of data localization measures in force worldwide more than doubled from 2017 to 2021(Cory & Dascoli, 2021); the high number of proposals today reflects the continued attraction of data localization policies to policymakers.

This legislation review found a wide spectrum of data localization policies globally in terms of the manner, scope, and stringency of their regulation. Of the 49 existing policies, excluding 18 proposals, about 65% (32 policies) were direct (explicit) policies, and about 35% (17 policies) were indirect (de facto) policies. China's Data Security Act, which took effect in the fall of 2021, is a representative example of direct policies; it requires "core data" ("broadly defined as any data that concerns Chinese national and economic security, Chinese citizens' welfare and significant public interests") and "important data" ("the next-most sensitive level of data, but its scope is left undefined") to be stored domestically (Junck et al., 2021, p. 1).

On the other hand, Australia's telecommunications interception laws, for example, can be categorized as an indirect policy. They "do not specify data sovereignty or data residency requirements, but do impose requirements on relevant providers to ensure interception capability or capacity exists in Australia and/or that there is some presence for law enforcement to deal with in Australia" and "may impact on decisions whether and how to offshore data and systems." (Baker McKenzie, n.d., Section b.)). Even if indirect policies appear to lack enforcement mechanisms, they often are as effective in forcing data localization as direct policies (Box 1).

Box 1 Guidelines can work as a data localization policy even without penalties.

There is no law in Japan requiring domestic storage of medical data. However, the Ministry of Health, Labour and Welfare (MHLW), which is in charge of Japan's healthcare administration, has published "Guidelines for the Secure Management of Medical Information Systems." The guidelines require that medical information and systems be stored in areas "subject to domestic laws" (Ministry of Health, Labour and Welfare of Japan, 2023, p. 68), which is understood to virtually require keeping medical information and systems in the domestic territory (Personal Information Protection Commission of Japan, n.d., A4-31, para. 2). So, this policy requests domestic data storage not by law but by guidelines without any penalties, which this paper classifies as an indirect (de facto) policy.

In an interview for the project, an executive of a Japanese medical institution said, "Since the guidelines are issued by the MHLW, which regulates the medical industry, the medical industry considers them to be almost like a law, and I think no medical institution thinks it is unnecessary to comply with them."

Among the policies sampled, soft data localization policies are the minority. These findings are consistent with those in a study led by the OECD; it refers to what this paper calls soft policies as "storage requirements" and further classifies hard policies into "storage and flow condition" and "storage and flow prohibition" and states two-thirds of the total data localization measures in 39 countries were "storage and flow prohibition" ones. (López González et al., 2022, pp. 7-8).

Many countries have implemented sector-specific data localization policies. This is a common trend among many countries, regardless of the geographic and economic differences among the sample jurisdictions. Of the 67 policies in the sample, 36% (24 policies) were data localization policies applicable to all sectors. Most of them were personal information protection laws (i.e., many countries subject personal information to protection regardless of industry). The remaining 64% (43 policies) were policies that applied only to specific sectors; most of them targeted four sectors: Financial Services, Information and Communications Technology (ICT), Public Sector, and Healthcare (Figure 2). The OECD study also lists "financial, banking or payments," "the public sector," and "telecommunications" as the top three sectors to which many data localization measures apply (López González et al., 2022, p. 10).

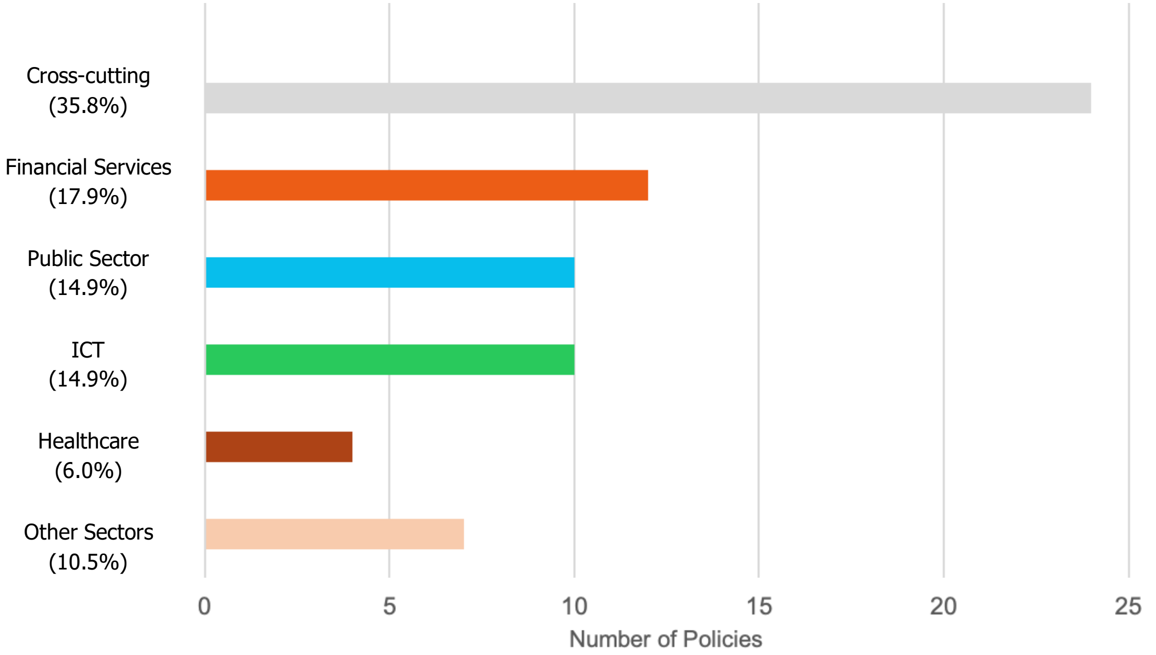


Figure 2 Percentage of Sector-specific Data Localization Policies[2]

In summary, the review found that many countries have a common legislative structure chosen from a wide spectrum of data localization policies. They establish data localization regulations for personal information without specifying industries and then establish even stricter data localization policies for specific sectors and data. On the other hand, some countries have introduced broad cross-industry data localization policies for data other than personal data, such as China's Data Security Act discussed above. In addition, this review found a number of data localization policies, while regulating data transfers outside the country, have exception clauses to their regulations, which can be considered as a common feature of policies as well. For example, the GDPR in the EU has the legitimate interest assessment (LIA) that, under stringent conditions, allows for the extraterritorial transfer of personal data even without fulfilling the requirements to do so (e.g., consent of the data subject) (Box 2).

[2] Source: Authors' compilation based on the 67 identified data localization policies.

Box 2 Companies may use the "legitimate interest" exception of the GDPR for information sharing in cyber incidents, which is, however, a very narrow path.

Article 44 of the GDPR permits the transfer of personal data outside the EU only if that transfer meets certain conditions set forth in the GDPR, such as if the destination country obtained an "adequacy decision" from the European Commission (Article 45) or if the data subject has given their explicit informed consent to that transfer (Article 49, 1. (a)) (Regulation (EU) 2016/679, 2016). However, the GDPR also provides for exceptional cases based on "legitimate interest" where data may be transferred abroad even if these conditions are not fulfilled (Article 49, 2.). According to the guidelines published by the European Data Protection Board on this provision, this legitimate interest exception "is envisaged by the law as a last resort" for situations where none of the other exceptions are applicable (European Data Protection Board, 2018, p. 14).

Specifically, "to transfer data under the legitimate interest exception, an organization needs to meet all of the following requisites" (Blair, 2018, Application of Article 49 Legitimate Interest Derogation Section):

1. The transfer is not repetitive
2. The transfer concerns only a limited number of data subjects
3. The transfer is necessary for the purposes of a compelling legitimate interest pursued by the controller that is not overridden by the interest or rights and freedoms of the data subject
4. The controller has provided suitable safeguards with regard to the protection of personal data
5. The controller informs the supervisory authority of the transfer
6. The controller informs the data subject of the transfer and the compelling legitimate interest pursued

Since this exception is "a last resort" that is only permissible in exceptional cases under stringent conditions, it is not something that companies can use for routine cyber threat information sharing. That said, in the commentary on the interpretation of the condition of "a limited number of data subjects," the guidelines used an example of a case where "a data controller needs to transfer personal data to detect a unique and serious security incident in order to protect its organization" (European Data Protection Board, 2018, p. 15). Therefore, in some situations, companies may consider using the legitimate interest exception in a cyber incident.[3]

[3] See also Recital 121 of the NIS 2 Directive (Directive (EU) 2022/2555, 2022).

3.2. Data Localization and Privacy

Data localization policies are designed to protect personal and sensitive data within a specific country, ultimately aiming to increase privacy protection. By restricting storing and processing of data to a defined location, these policies provide governments with greater autonomy to regulate and control data. The rationale behind these policies is that personal and sensitive data within domestic territories becomes inaccessible to foreign legal authorities. Thus, by safeguarding data from external parties and imposing regulations on data processing by other stakeholders, governments with data localization policies aim to enhance privacy protection.

Moreover, as it is underlined in the NIST's Special Report (2016), "multinational corporations need to consider the differences in various nation's privacy laws and how to address handling of classified information, which typically cannot be shared with foreign nationals" (Johnson et al., 2016, p. 10). As such, data localization policies do not only control the access of personal and sensitive data by legal authorities of other nations but also limit the reach of multinational companies by putting additional restrictions on these companies. This helps to reduce unauthorized access to data which is expected to help protect privacy.

Nevertheless, the consequences of those policies on security do not always result in benefits for privacy interests. This means that although the main objective of data localization policies is often to protect privacy, their real impact may not always serve this purpose due to their side effects on cybersecurity. In one of the interviews, Lily Fang, Chief Privacy Officer at Palo Alto Networks (personal communication, March 6, 2023), underlined that "protecting personal data and ensuring privacy is only possible with a strong cybersecurity posture within the company". While her argument highlights the importance of cyber resilience for privacy protection, it also underscores how privacy and security are mutually reinforcing concepts. Both aim to prevent unauthorized access and safeguard personal information, making them complementary objectives.

In interviews conducted with cybersecurity experts, the majority of the interviewees agreed that although data localization policies in many jurisdictions are intended to protect privacy, they can also create complexities in cybersecurity. **If data localization policies with privacy concerns make it more difficult to identify and mitigate a cyber-attack, then it increases the cyber risks and hampers cybersecurity.**

3.3. Data Localization and Cybersecurity

In this section of the paper, the main hypothesis on data localization and cybersecurity, which is that data localization requirements have a negative impact on the cross-border sharing of cyber threat information, will be examined in detail through a literature review, expert interviews, and case studies.

3.3.1. How does data localization affect cybersecurity?

Data localization policies are designed to limit the cross-border flow of personal (and sometimes non-personal data as well) to enhance privacy protection and provide greater autonomy in the use of data. They also significantly impact cybersecurity. For example, Swire and Kennedy-Mayo (2022) analyzed that data localization negatively affects 13 out of the 14 ISO 27002 controls, the international standard for information security that represents the best-in-class cybersecurity measures. Some of the consequences of data localization policies relate to technologies, while others link to specific regulatory mechanisms in each country. In order to elaborate on these various aspects of impacts, this section will address the most significant issues concerning cybersecurity, which may arise from data localization policies.

Geographical restrictions on data location cannot prevent cyberattacks from remote areas.

While data localization policies directly relate to privacy protection, their contribution to cybersecurity is hard to define. Some data localization policies intend to protect privacy by securing greater autonomy to regulate and control data. However, in an interview, Neal Pollard, Partner at EY, argued, “Although certain data is not reachable by other nations’ legal authorities, it is still reachable by hackers, intelligence officers, and unethical competitors” (Neal Pollard, personal communication, March 6, 2023). As Pollard points out, the geographical locations of data themselves do not have much meaning in preventing systems from being breached and data from being stolen.

Furthermore, the findings from various interviews and research in the study support that there is no clear correlation between the strictness of a country’s data localization policies and the robustness of cybersecurity. In fact, several use cases suggest that data localization makes it more difficult to prevent cyber threats and restore cybersecurity in some circumstances.

Data localization policies implementing geographical limitations prevent using cloud storage.

These policies can decrease security and resilience in cloud services by limiting the number of data centers where personal or sensitive information can be stored. Some computer experts emphasized the importance of global cloud storage centers and sharding technologies, stating that "Requirements to localize data (...) only make it impossible for cloud service providers to take advantage of the Internet's distributed infrastructure and use sharding and obfuscation on a global scale" (Ryan et al., 2013, p. 57).

Even if companies have different data centers that can provide cloud services in different locations, they are not allowed to store the data at data centers outside of the country with data localization policies. This restriction creates a high risk of a single attack taking out all data when there is only one data center within the same jurisdiction. In an interview, Pam Kingpetcharat, Lecturer, School of International and Public Affairs, Columbia University, highlighted that data localization requirements in some countries prohibit the use of cloud storage services such as Box or Dropbox if the data is stored outside the country, effectively creating a physical barrier that can undermine cybersecurity efforts by limiting the range of tools and services available to support security efforts (Pam Kingpetcharat, personal communication, March 3, 2023). In parallel with cybersecurity arguments, Neal Pollard also addressed that data localization policies erode cyber resilience in cloud services by restricting the number of data centers where a piece of personal information is kept (Neal Pollard, personal communication, March 6, 2023). In particular, data localization policies pose a significant risk of data theft in small countries where companies tend to have only one data center.

Thus, data localization policies not only undermine cybersecurity in cloud services but also increase cyber threats and limit the ability to establish strong cyber resilience. It cuts companies off from advanced cloud-based third-party security services. A compelling example of how data localization policies decrease cybersecurity can be observed in the case of Cloudflare in Portugal (see 3.4.1.).

3.3.2. How does data localization inhibit information sharing?

The borderless nature of cyberattacks and their growing frequency and sophistication can be best addressed with cyber threat information sharing. In order for companies to detect and respond to cyberattacks, the information they receive from their companies and other organizations is key. Government agencies such as the United States Cybersecurity & Infrastructure Security Agency and the European Union Agency for Cybersecurity (ENISA) have identified information sharing as essential to improving the world's cybersecurity risk posture (CISA, 2016; ENISA, 2015).

As highlighted by NIST, **cyber threat information** includes "any information that can help an organization identify, assess, monitor, and respond to cyber threats. Cyber threat information includes indicators of compromise; tactics, techniques, and procedures used by threat actors; suggested actions to detect, contain, or prevent attacks; and the findings from the analyses of incidents" (Johnson et al., 2016, p. iii). Cyber threat information sharing gives organizations access to threat information and situational awareness of the current threat landscape. Additionally, information sharing allows organizations to utilize the knowledge, experience, and capabilities of others, enhancing their security and defense agility (Johnson et al., 2016). This sharing and collaboration across organizations, sectors, governments, and borders create greater resilience against increasingly sophisticated cyber-attacks.

By exchanging cyber threat information, organizations can leverage their collective knowledge, experience, and capabilities to gain a more complete understanding of the threats organizations may face. By using this knowledge, organizations are able to make threat-informed decisions regarding defensive capabilities, threat detection techniques, and mitigation strategies. By correlating and analyzing cyber threat information from multiple sources, an organization can also enrich existing information and make it more actionable.

Data localization policies may hinder the cross-border sharing of cyber threat information.

Data localization disrupts information sharing as such measures put restrictions on the free flow of data. If there are required localization laws in two or more countries, this hinders the ability to conduct integrated cybersecurity management - including information sharing of emerging cyberattacks, trend analysis, and forensics concerning data breaches. Data localization poses this risk to cyber threat information sharing because it sets restrictions on a broad set of data, such as personal data. Often falling under the category of personal data, and thus falling victim to data localization policies, is security data. Security data, which is critical to an organization's ability to protect and defend itself from cyber threats, includes device, network, and endpoint information as well as other information such as URLs/Domains, session data, threat intelligence or data, statistics, aggregated data, NetFlow data, and in some cases, includes personal data that is necessary for the furtherance of security (i.e., hyperlink to a malicious website or a malicious IP address) (Palo Alto Networks, 2022a).

Localization measures targeting a broad scope of data - like personal data - consequently limit the sharing of security data amongst critical information-sharing services, including services that monitor for cyberattacks and provide threat analysis and threat prevention (Swire & Kennedy-Mayo, 2022). This not only impacts a single organization's cybersecurity but disrupts information sharing that is leveraged globally for collective knowledge, experience, and capabilities in order to gain a more complete understanding of the global cyber threat landscape.

Regarding the negative consequences of data localization laws on cybersecurity, the findings of Swire and Kennedy-Mayo (2022) suggest that "Although good cybersecurity practice integrates management of the organization's system, required localization in two or more nations restricts the ability to conduct integrated cybersecurity management – including information sharing of emerging cyberattacks, trend analysis, and forensics concerning data breaches," (p.5). While keeping data in a defined location not only debilitates cybersecurity, it also hinders global cooperation by preventing cross-border data flows. This limitation on information sharing hampers cooperation between multinational corporations, private-public entities, and private-private entities. It slows down the cyber-attack mitigation process and hampers cybersecurity management.

Data localization destroys the firms' capabilities of data aggregation key to developing advanced analytics using machine learning.

Data localization policies, however, have a negative impact on data aggregation and machine learning technologies, which are increasingly becoming integral parts of establishing cybersecurity. Swire and Kennedy-Mayo (2022)'s findings agree that "cybersecurity increasingly relies on machine learning, artificial intelligence, and other automated techniques to detect and respond to cyberattacks" (p. 23). Machine learning, which is used to enhance advanced analytics, relies heavily on data aggregation. Companies that want to advance in machine learning capabilities must be able to aggregate large and diverse data sets.

However, as an incident response professional pointed out in an interview, data localization policies can hinder this process by restricting the ability to store data in different locations, leading to a fragmented data set that makes it difficult to extract meaningful variables necessary for advanced analytics. These policies also may hinder the detection of potential useful patterns, which can only be found using data from various countries.

Furthermore, In incident response and forensic investigations, a process known as "stitching" is used to identify the root cause of a security incident, help track the spread of a threat, and determine the extent of the damage. This process involves combining different pieces of information to obtain a comprehensive view of a security event or incident and involves analyzing data from multiple sources, such as network logs, system logs, and security devices. If there are data localization requirements in place preventing the movement of data, especially security data, this will frustrate the ability to stitch together features of incidents that cross multiple geographies since stitching exercises require all logs from the incidents to be in a common location.

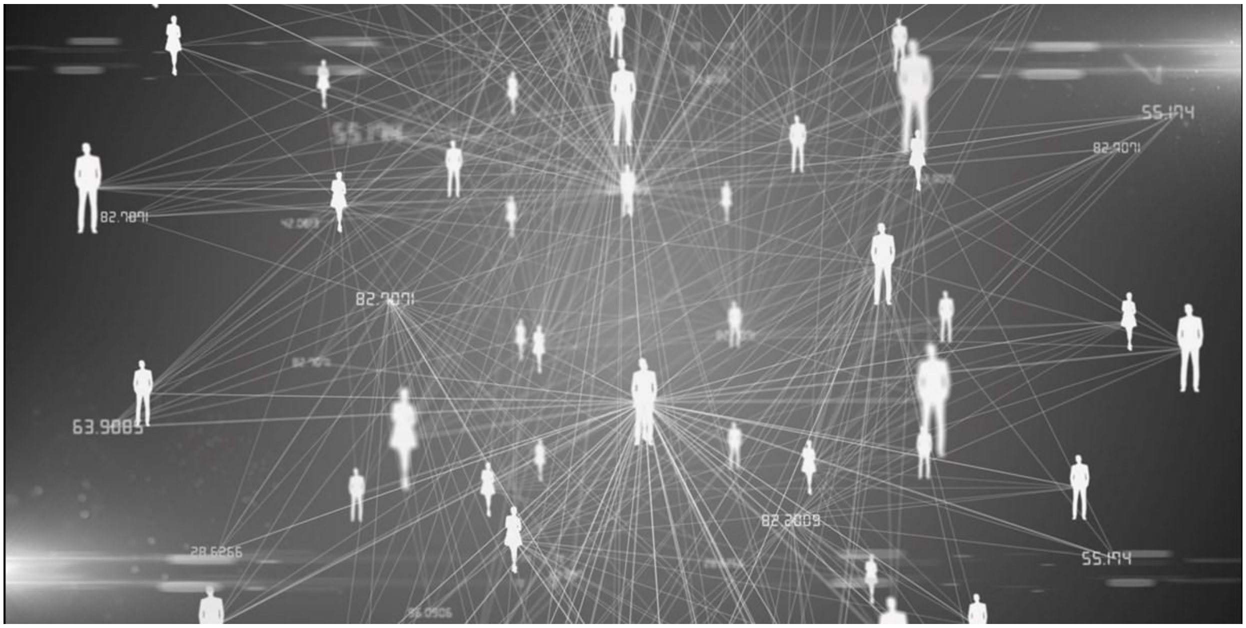
Another aspect of this argument raised by the incident response professional is that feature extraction in machine learning is based on the rawest form of data, and whenever data is aggregated or trimmed, it frustrates the ability to extract meaningful variables from that data set. Additionally, any relationship that could be discovered with feature extractions is not possible if data is isolated or segregated. This can cause a huge financial and human capital burden, as people would have to manage things such as writing and managing software. Essentially, every time someone writes a piece of software, they must take into account the limitations of data localization policies, which can hinder their ability to aggregate and analyze data effectively.

Therefore, data localization policies put serious constraints on data aggregation and destroy the ability of companies to utilize machine learning. Furthermore, it can be arguably claimed that it leads to a lack of advanced analytics in the field of security.

3.4. Use Cases

3.4.1. Cloudflare for 2021 Portugal Census

In April 2021, The Portuguese National Data Protection Commission (CNPD) ordered the Portugal National Institute of Statistics (INE or Statistics Portugal) to stop using Cloudflare, a California-based cloud network delivery (CND) provider, to process the census 2021 within a 12-hour compliance window (CNPD, 2021). This GDPR enforcement case demonstrates how the EU's gravitation towards data localization disrupts a multinational company's ability to share cyber threat information across the EU and the US (Kennedy-Mayo & Swire, 2021).



Cloudflare's relationship with Statistics Portugal drew scrutiny because it is an American company processing sensitive personal information of the Portuguese population (6.5 million data subjects collected at the time of the order). While CNPD recognized that Cloudflare services fulfill a legitimate purpose (to ensure the efficiency and security of the online fulfillment of the survey), it argued that INE's contract with Cloudflare violates GDPR in the light of CJEU judgment in the Schrems II case, which found that data transfers to the US are inadequately protected from US government surveillance risks (CNPD, 2021). In December 2022, CNPD found five GDPR violations and levied a fine of 4.3 million euros in December 2022 (European Data Protection Board [EBPD], 2022). Two of the five GDPR violations found by CNPD used data localization language: "lack of due diligence concerning the choice of the processor (Article 28(1),(6) and (7))" and "lack of compliance with the legal requirements for international data transfers (Articles 44 and 46(2))" (EBPD, 2022, Key Findings).

Statistics Portugal was accused of not knowing the data's exact locations once the census data entered Cloudflare's network (EBPD, 2022). However, this statement shows a lack of understanding of cloud services: Cloudflare is designed to optimize performance and storage by scattering data around its more than 200 data centers worldwide (Cloudflare, n.d.).

Third-party cybersecurity services, such as Cloudflare, prevent malicious activities like DDoS attacks, malicious bots, and other nefarious intrusions by sharing cyber threat information across its globally distributed data centers (Cloudflare, n.d.). Data localization policies are at odds with the nature of cyber threat intelligence, which identifies patterns of threat actors by moving any information about threat actors across different organizations and countries. Neal Pollard, Partner at EY (personal communication, March 9, 2023), pointed out that **being cut off from these services can leave organizations vulnerable to cyber-attacks and limit their ability to respond effectively to such attacks**.

3.4.2. Palo Alto Networks Unit 42 - Chinese APT "GALLIUM"

In June 2022, Palo Alto Networks' Unit 42 team released a report that IDs a known Chinese advanced persistent threat (APT) and highlights not only the group's development of a new remote access trojan (RAT) but also the expansion of targets beyond the primary sector that the group has been known to attack.

According to the analysis by Unit 42, "GALLIUM (also known as Softcell), established its reputation by targeting telecommunications companies operating in Southeast Asia, Europe, and Africa. The group's geographic targeting, sector-specific focus, and technical proficiency, combined with their use of known Chinese threat actor malware and tactics, techniques and procedures (TTPs), has resulted in industry assessments that GALLIUM is likely a Chinese state-sponsored group" (Palo Alto Networks, 2022b, Executive Summary para. 2).

From 2021 to 2022, Gallium extended its targeting beyond telecommunication companies to also include financial institutions and government entities. During the course of that year, Unit 42 identified several connections between GALLIUM infrastructure and targeted entities across Afghanistan, Australia, Belgium, Cambodia, Malaysia, Mozambique, the Philippines, Russia, and Vietnam. Even more critical, Unit 42 also identified the group's use of a new and previously undocumented remote access trojan (PingPull) that mimics legitimate computer activity, making it harder to detect. The malware can perform a variety of activities once inside a system, such as reading, writing, deleting, copying, and moving files (CyberScoop, 2022).

Leveraging cyber threat information shared from all around the world and among different entities (such as Cybersecurity Collaboration Center, the Australian Cyber Security Centre, and other government partners), Unit 42 detected GALLIUM's movement and use of PingPull. For example, in September 2021, an organization in Vietnam shared a sample of PingPull with the cybersecurity community. Analysis of the sample revealed that it was configured to report network location, username, or other data to a remote "home" server: t1.hinitial[.]com. Unit 42 identified additional subdomains hosted under the initial[.]com domain, and identified overlaps in certificate use between the various IP infrastructure associated with each of the subdomains.[4] The PingPull samples and their associated command and control domains led to the identification of over 170 IP addresses associated with this group dating back to late 2020.

The discovery of GALLIUM's target expansion and use of PingPull exemplify the necessity of cyber threat Intelligence (CTI) sharing. In the GALLIUM discovery, by identifying targets and patterns by the group, in addition to detecting the PingPull malware, Unit 42 and partners were able to provide a warning on this active threat as well as indicators of compromise (IoCs) that help identify if an origination has been impacted. From there, organizations have the information necessary to mitigate any potential threat and enhance defensive cyber capabilities.

The introduction of data localization policies has consequential impacts on CTI and information sharing. According to Jen Miller Osborn, Head of Strategic Engagement and Analysis for Unit 42, **data localization would completely prohibit the type of analysis and work done in the GALLIUM report**. Overall, data localization policies would prohibit the sharing of data and debilitate the entire cyber threat intelligence process (Jen Miller Osborn, personal communication, March 21, 2023).

Security data such as IP addresses often fall under the category of personal data, of which many data localization policies restrict the cross-border movement. In the GALLIUM case, if Unit 42 and

[4] Command and control is a technique used by threat actors to communicate with compromised devices over a network.

its partners were not able to share security data like the IP addresses from different jurisdictions that were able to identify the process of PingPull, it is likely that the malware would have remained undetected and undocumented, therefore allowing GALLIUM to continue its espionage attacks in multiple countries.

3.5. Private Sector Response

The growing number of data localization measures and proposals, and their implications for cybersecurity, are of concern for the private sector. The goal of cybersecurity is not only to protect against and keep threat actors out of networks but also to protect the privacy of customers. By limiting the use of strong DDoS mitigation programs, hindering threat intelligence sharing, and preventing the dissemination of warnings about potential cyber threats, the private sector faces more vulnerability as cybersecurity is weakened due to data localization measures. Consequently, weakened cybersecurity leaves one more susceptible to cyberattacks and affects the ability to protect people’s privacy.

On top of impacts to cybersecurity, data localization measures create the following additional obstacles for the private sector:

Cost

While data localization measures may differ, they all ultimately would have a cost component, creating extraneous overhead associated with every type of localization, even the most benign type, according to an incident response professional. For instance, in cases where a company must leave a copy of data in country X, they will also have to pay fees associated with the storage of the data. All administrative activities come from the same pool of corporate funds; therefore, the more a company has to spend on its legal team due to the increased burden of data localization policies, theoretically, the less it can spend on cybersecurity (Daniel Dobrygowski, personal communication, March 1, 2023). Additionally, when more than two countries or regions require localization, organizations are faced with having to segregate their networks in various ways depending on the nation and type of data (Swire & Kennedy-Mayo, 2022). Such a task requires organizations to allocate resources and funds to deal with it. This specifically puts pressure on smaller cybersecurity enterprises that may not have the funding and often cannot operate in certain countries or regions with data localization policies. Lastly, if cyber defense companies are debilitated by data localization policies, this increases the risk of cyberattacks that can come with steep financial burdens.

Compliance

Companies are focused on ensuring that they are complying with the array of national laws and regulations in the countries they do business. Compliance generally is a business enabler; however, with sometimes contradictory data localization measures, compliance becomes complicated. As more countries and regions create data localization policies, organizations end up facing more conflicts of law (Swire & Kennedy-Mayo, 2022). This is because situations arise where one country's law requires that data must be transferred to that country (i.e., for accounting or regulatory oversight) while another country's law says the transfer is unlawful. This creates a dilemma for companies in terms of compliance because by complying with one country's law, they could be ultimately breaking another's. The fragmented landscape, therefore, makes it difficult for companies to not only comply sufficiently with local laws but also difficult for these companies to operate.

Time

Real-time sharing of cross-border threat data is key to strong network defense, cyber intelligence analysis, and an organization's ability to comply with other laws within a country's jurisdiction. Attackers quickly identify system vulnerabilities and weaknesses; therefore, in a cyber environment where threat actors share information quickly, the timeliness in which security data is received is essential for organizations to stay competitive and secure (Jason Harrell, personal communication, March 24, 2023). **It is not enough that data be shared; the data also must be useful.** For instance, in cyber threat intelligence, necessary cross-border sharing of security data must be shared within a 30-60-90 days window; any information shared past 90 days becomes less valuable (Jen Miller Osborn, personal communication, March 21, 2023). Additionally, in network defense, any delay in data ingestion inhibits not only the detection and investigation of a threat but also prevents the dissemination of warnings about potential cyber threats to others at risk. For example, a large bank in a data localization geography would be unable to send warnings about potential cyber threats to relevant client advisors in other countries (Neal Pollard, personal communication, March 6, 2023). Lastly, delays in sharing and ingesting data ultimately impact an organization's ability to adhere to other laws, such as those with mandatory notification periods reporting a breach or incident.

4. Regulatory Frameworks

The analysis above clearly articulates that data localization negatively impacts cybersecurity by inhibiting necessary information sharing and imposing troublesome burdens on entities in the private sector.

That said, the need for data protection policies is, however, widely recognized throughout the world. To protect the personal information of citizens is obviously a legitimate policy objective. Many countries today have data protection laws, and as stated in Section 3.1, many of them have de facto effects as data localization policies. In this context, eliminating data protection policies around the globe to enhance cybersecurity is no longer a realistic and appropriate option.

Therefore, given the existence of data localization policies, the paper will proceed to discuss what regulatory framework for data protection best considers and balances privacy and security interests.

4.1. Existing Regulatory Frameworks

The analysis in Section 3. has revealed a wide range of data localization policies that are being implemented globally, highlighting the need for a consensus to strike a balance between privacy protection and cybersecurity to maintain trust and safety in the digital environment.

In order to address this challenge, regulatory frameworks have been established by some international and regional organizations, such as the European Union (EU) and Asia-Pacific Economic Cooperation (APEC). These frameworks, such as the General Data Protection Regulation (GDPR) and Cross-Border Privacy Rules (CBPR), have been designed to address data protection and global data transfer. GDPR is a comprehensive data privacy regime that came into effect in May 2018. It sets out rules for EU members with extraterritorial implications. The GDPR builds on previous EU data protection rules and introduces new rights for individuals to control their personal data while establishing specific new data protection requirements. The APEC CBPR is a privacy code of conduct established in 2011 that aims to protect personal data and enable cross-border data flows between its members. The APEC framework identifies best practices that each member can tailor to its own legal system, allowing for flexibility in implementation mechanisms and scope (Fefer, 2020).

To help understand existing regulatory frameworks for global data transfer, the United Nations Conference on Trade and Development (UNCTAD) has categorized their approaches based on their exceptions(UNCTAD, 2016).

4.1.1. One-off Exceptions

According to a report by the International Centre for Policy Leadership, the following one-off exceptions are the most common (Hunton & Williams LLP, 2015):

- The transfer is necessary for the performance of a contract between the data subject and the controller or between the controller and a third party, and (i) is entered into at the request of the data subject, or (ii) is in the interests of the data subject;
- The transfer is for the purpose of legal proceedings, for the purpose of obtaining legal advice, or for establishing, exercising, or defending legal rights; or
- The transfer is necessary in order to protect the vital interests of the data subject.

This is not an exhaustive list, but it does demonstrate the current 'common ground' in national privacy laws. As discussed previously, the approach of one-off exceptions, however, is a very narrow path and can be impractical for daily cybersecurity usage (See Box 2 in Section 3.1.2.). Therefore, to better balance privacy interests and cybersecurity, the regulatory frameworks should implement the ongoing exceptions, which are discussed in the next section, for cyber threat information sharing and other cybersecurity-related activities.

4.1.2. Ongoing Exceptions

The utilization of ongoing exceptions exhibits a lack of uniformity. There is no consensus or agreement at the global level regarding their implementation, as shown by the following list.

- **The "adequacy" approach:**
  (also known as a whitelist approach): The "adequacy" approach evaluates whether a target jurisdiction as a whole offers an adequate level of protection for the transfer of personal data. This methodology is employed by several countries, including members of the European Union (EU), Israel, Japan, and Switzerland.

- **The "binding rules" approach:**
  The "binding rules" approach pertains to the evaluation of whether a particular company has implemented procedures and autonomous review mechanisms that guarantee a satisfactory level of protection for the transfer of personal data, usually within the larger corporate group. This methodology is employed in the European Union's Binding Corporate Rules system (BCRs). Several individual jurisdictions have the capacity to acknowledge such binding rules, specifically Australia and Japan.

- **The "model contracts" approach:**

The "model contracts" approach, also called "Standard Contractual Clauses (SCCs)," evaluates whether the specific language used in contracts offers an adequate level of safeguarding for the transfer of personal data. Different jurisdictions have varying legal authorities when it comes to model contract frameworks for international transfers of personal information. Some jurisdictions acknowledge these frameworks at a national level, often in accordance with national data protection laws that restrict entities' ability to transfer personal information abroad.[5] This methodology is employed in the EU, the Association of Southeast Asian Nations (ASEAN), and the Ibero-American Data Protection Network (Matheson, 2023).

- **The "consent" approach:**
  The "consent" approach assesses the ability of individual consumers to give consent for the transfer of their data to a foreign country. Although this approach is utilized in the European Union's GDPR (Intersoft consulting, n.d.) and some other jurisdictions, it is also subject to additional requirements pertaining to the nature of the consent.

- **The "accountability" approach:**
  The "accountability" approach seeks accreditation from an approved third-party organization, known as an "Accountability Agent." The APEC CBPR Certification is a mechanism to facilitate cross-border data transfers by organizations. It has been likened to BCRs in the EU but with a broader scope (Centre for Information Policy Leadership, 2020). The Accountability Agent is supposed to certify the organization and recertify them each year. Once deemed compliant, organizations are included in a compliance directory. Organizations are subject to potential enforcement, through law or contract, by Accountability Agents and also privacy enforcement authorities in participating economies (APEC, 2018).

4.2. How Existing Regulatory Frameworks Address Cybersecurity Issues

This section has identified five crucial criteria for evaluating the strengths and weaknesses of different approaches toward establishing a global consensus on regulatory frameworks for cybersecurity and data privacy.

[5] For example, the Republic of the Philippines National Privacy Commission (2021) stated, "ASEAN MCCs may also be used by companies or organizations to fulfill…obligations under Section 21 of the DPA" (p. 3).

4.2.1. Criteria

1. **Interoperability:** To what degree do privacy regimes or legal frameworks work together to facilitate transborder data flows while ensuring the consistent protection of data (OECD, 2021).
2. **Timeliness:** To what extent does a framework allow for timely cyber threat information sharing.
3. **Persistency:** How consistent is the regulatory framework. A regulatory framework that is persistent is more likely to be effective over the long term, as it provides legal certainty and predictability to those involved in cyber threat information sharing (Nigel Cory, personal communication, 2023).
4. **Transparency:** How transparent are the processes for creating the regulatory framework, including the drafting of rules and regulations, public consultation, and stakeholder engagement. How transparent are the processes organizations use in data collection and processing (Nigel Cory, personal communication, April 11, 2023).
5. **Enforcement:** Is there a well-resourced, effective enforcement mechanism in place. Inadequate enforcement may lead to increased violations and distrust of the regulatory framework.

4.2.2. Evaluation based on the Criteria

Based on the evaluation criteria established, this section assesses the above approaches and presents the findings. Table 2 shows the overview of the evaluation, and Table 3 indicates the details.

Table 2 Evaluation of The Approaches Based on the Criteria (Overview)

		Approaches				
		Adequacy	**Binding Rules**	**Consent**	**Model Contracts**	**Accountability**
Criteria	**Interoperability**	Weak	Moderate	Moderate	Strong	Strong
	Timeliness	Moderate	Moderate	Weak	Moderate	Strong
	Persistency	Weak	Strong	Strong	Weak	Strong
	Transparency	Weak	Strong	Strong	Weak	Strong
	Enforcement	Weak	Weak	Moderate	Strong	Moderate

Table 3 Evaluation of The Approaches Based on the Criteria (Details)

	The "adequacy" approach	The "binding rules" approach	The "consent" approach	The "model contracts" approach	The "accountability" approach
Interoperability	**Weak** This approach makes it difficult for countries to reach the high bar set by GDPR and EU jurisprudence.	**Moderate** The approach for effective data protection in the private sector is restricted to large groups and duplicates approval procedures.	**Moderate** It provides a common set of standards for obtaining consent across jurisdictions. However, it may not be sufficient to address more complex issues.	**Strong** SCCs are one of the most widely used mechanisms by the U.S., EU, and other firms—from a broad range of sectors to transfer personal data.	**Strong** It can provide a basis to scale up because it reflects economies at different stages of development and includes industry participation.
Timeliness	**Moderate** It enables timely transfer for those countries found adequate; however, the process to determine adequacy is lengthy.	**Moderate** The approach enables a free flow of data within a corporate group; however, the approval process is excessively long.	**Weak** It may take time to obtain consent from data subjects before sharing their data.	**Moderate** Model contracts can cause transfer delays, but pre-approved models can still expedite the process compared to bespoke agreements.	**Strong** It enables a free flow of data within certificated organizations, and the certification process is relatively fast and less costly.
Persistency	**Weak** It exhibits inconsistencies, as major trading partners receive partial determinations despite established data protection frameworks.	**Strong** The BCRs are seen as the 'gold standard' for compliance and can be tailored to fit the needs of the business.	**Strong** Once consent is obtained, it can provide legal certainty and predictability to those involved in cyber threat information sharing.	**Weak** It is challenging to develop appropriate model clauses in the face of evolving data protection laws and to keep organizations up to date.	**Strong** Certification can serve as a readily identifiable indication of a company's dedication to privacy and responsible management of data.
Transparency	**Weak** Many countries that use a whitelist approach fail to develop and use clear, common, and consistent criteria for listing or delisting countries.	**Strong** The BCRs must have clauses on liability and data protection principles; information must be provided in full (or providing links to privacy policies, etc.).	**Strong** It involves obtaining explicit consent from data subjects regarding the transfer of their personal data.	**Weak** No transparency about who is using model clauses.	**Strong** Following certification, the organization is entered into a compliance directory, which can enhance transparency in an objective way.
Enforcement	**Weak** Complying with the changing standards is difficult, and businesses may not find adequacy useful if its scope is limited.	**Weak** The application and approval process is burdensome and excessively long, leaving organizations in legal limbo in the interim.	**Moderate** While it has a low compliance burden, the potential risk of unfairness for the power imbalance between the parties cannot be ignored.	**Strong** It can be quickly implemented by individual businesses willing to adopt the model contractual clauses verbatim.	**Moderate** Enforcement may be challenging due to jurisdictional issues and lack of resources in developing economies.

4.3. Policy Recommendations

4.3.1. Evaluation Results of Regulatory Frameworks

The "accountability-based" approach, exemplified by the APEC Cross-Border Privacy Rules (CBPR) System, is a pragmatic regulatory framework that balances privacy and security interests, especially cross-border cyber threat information sharing.

The "accountability-based" approach receives the highest score in addressing concerns related to interoperability, timeliness, persistence, and transparency, while also demonstrating a moderate level of enforcement.

Therefore, this paper encourages the recognition of the "accountability-based" approach of the CBPR. The evaluation found the interoperability and persistency of this approach because the CBPR system's advantage is that it allows for transfers not only within a global corporate group but also between non-affiliated companies, and data can also be transferred to companies that are not CBPR-certified between participating APEC economies. Regardless of the data's destination, the CBPR-certified company is responsible for safeguarding the information at the level of the originating APEC country and the CBPR. Moreover, the "accountability-based" approach prioritizes transparency and enforcement, which makes it feasible for companies to participate. This paradigm also emphasizes the timeliness to ensure on-demand cyber threat information sharing, which is crucial for maintaining cyber resilience.

Countries outside of APEC that implement comparable mechanisms could make their cross-border regulations compatible with the CBPR and other comparable initiatives. This would establish a universal certification mechanism to cover a large number of economies.

4.3.2. Future Policy Engagement and Research

To shape the regulatory frameworks and their translation into national policies regarding international data transfers, cybersecurity stakeholders can consider the following options:

1. **Highlight cybersecurity policy objectives hindered by data localization by participating in multistakeholder forums through tech trade associations and investing in cybersecurity coalitions.**

   - A multistakeholder approach is essential because data transfers and cybersecurity are complex and affect the entire cybersecurity ecosystem. "No one entity understands the entirety of the space," says Daniel Dobrygowski, Head of Governance & Trust at the

World Economic Forum (WEF), who encourages a detailed look at how laws interact (Daniel Dobrygowski, personal communication, March 1, 2023). In fact, the Japanese Economic Ministry acknowledged that "regulations that are seemingly resulting from a lack of understanding of the business reality regarding data transfer to third countries" increase costs for cross-border transfer of data (Ministry of Economy. Trade and Industry of Japan, 2022, p. 44). A WEF white paper suggests that a multistakeholder track that gathers institutionalized communities of technical experts, industry representatives, and civil society organizations can enrich intergovernmental processes and digital trade avenues on global data governance (Drake, 2018, p. 14).

- Trade associations and cybersecurity coalitions are good avenues for individual organizations to participate in multistakeholder policy-making processes. Several cybersecurity professionals interviewed in this study are familiar with trade associations' initiatives to push for regulatory harmonization on policies that affect them. Furthermore, to increase the weight of the cybersecurity perspective, a dedicated cybersecurity coalition that shares the pain points regarding cyber threat information sharing and cyber resilience can be a force multiplier.

2. Encourage internal and industry-wide publication of case studies highlighting how data localization harms critical cross-border threat information sharing.

- Organizations should publish more use cases like the two in Section 3.4 to show how linking threat data across countries achieves cyber defense objectives and how data localization policies threaten to destroy this ability. Forcing "geographic limits around a problem that does not respect geography" hinders a company's ability to hunt for the very threats that worry regulators, as Yoel Roth, former Head of Trust and Safety at Twitter, wrote about TikTok's plan to air-gap US user data (Roth, 2023, para. 17). The storytelling of use cases can be more effective at persuading regulators and help properly scope policies.

- Within an organization, policy professionals can identify use cases from security teams, especially incident response and endpoint professionals, who are most likely to be impacted by the reduction in available threat information and capabilities to aggregate data.

- Industry-wide sharing of use cases can strengthen the cybersecurity coalition in cross-border data governance. Currently, these use cases may be limited to trusted circles, but sharing the benefits of cross-border cyber information sharing can help counter the misguided narrative that puts privacy and cybersecurity at odds.

3. **Future research topics include mapping the stakeholders, aggregating industry comments to policy proposals, and developing metrics to quantify the impact.**

   - Identifying stakeholders of varying sizes, geography, and sectors requires more research. In a two-month timeline, this team conducted 16 interviews, including industry experts from healthcare, financial services, technology, and nonprofit sectors and policy experts from academia, think tanks, and international organizations. Future research efforts should include a longer interview timeline and a representative pool of interviewees. Once a fuller spectrum of stakeholders is identified, a future research effort can probe into the sources of use cases and barriers to sharing these stories.

   - Reviewing comments submitted to proposed data localization policies is a valuable research avenue that the scope of this paper could not accommodate. Following Swire and Kennedy-Mayo (2022)'s methodology of reviewing around 200 comments submitted to European regulators about data transfers (pp. 9-10), the same type of analysis should be done with comments submitted to other regulators as it is an active space for legislation. This exercise may also reveal which voices are not being heard, such as micro, small, and medium-sized enterprises (MSMEs) and nonprofit organizations not as well-resourced to submit comments and participate in global forums (Drake, 2018, p. 5).

   - Finally, better metrics for domestic cyber resilience are required to measure the effects of data localization. The cybersecurity industry is increasingly shifting from traditional cybersecurity management to a more proactive cyber resilience framework (Alcove, 2021), but more consensus is needed on measuring cyber resilience. An example is BIS's Principles for Operational Resilience for banks (Basel Committee on Banking Supervision, 2021). A future study can seek practical cyber resilience metrics that help organizations demonstrate how different data transfer policies affect business operations.

Reference

Alkove, J. (2021, November 3). *Why we need to move from cyber security to cyber resilience*. World Economic Forum. https://www.weforum.org/agenda/2021/11/why-move-cyber-security-to-cyber-resilience/

Asia-Pacific Economic Cooperation. (2021, October). *What is the Cross-Border Privacy Rules Systems.* Retrieved April 30, 2023, from https://www.apec.org/About-Us/About-APEC/Fact-Sheets/What-is-the-Cross-Border-Privacy-Rules-System.

Baker McKenzie. (n.d.). *Australia.* Resource Hub. Retrieved April 30, 2023, from https://resourcehub.bakermckenzie.com/en/resources/data-privacy-security/asia-pacific/australia

Basel Committee on Banking Supervision. (2021, March 31). *Principles for operational resilience*. Bank for International Settlement. Retrieved April 28, 2023, from https://www.bis.org/bcbs/publ/d516.htm

Cawthra, J., Ekstrom, M., Lusty, L., Sexton, J., Sweetnam, J., & Townsend, A. (2020). *Executive Summary—NIST SP 1800-25 documentation*. Retrieved April 28, 2023, from https://www.nccoe.nist.gov/publication/1800-25/VolA/index.html

Centre for Information Policy Leadership (CIPL). (2017). *Cross-Border Data Transfers: A Review of Selected Mechanisms (White Paper)*. Hunton & Williams LLM. Retrieved April 30, 2023, from https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cross-border_data_transfers_mechanisms_cipl_white_paper.pdf

Centre for Information Policy Leadership (CIPL). (2020). *APEC, CBPR & PRP Questions and Answers*. CIPL Cross-Border Privacy Rules and Privacy Recognition for Processors FAQs. Hunton & Williams LLM. Retrieved April 30, 2023, from https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2020/03/cipl_cbpr_and_prp_q_a_final__19_march_2020_.pdf

Centre for Information Policy Leadership (CIPL). (2023, March 29). *The "Real Life Harms" of Data Localization Policies*. Hunton & Williams LLM. Retrieved April 30, 2023, from https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl-tls_discussion_paper_paper_i_-_the_real_life_harms_of_data_localization_policies.pdf

Cloudflare. (n.d.). *What is Cloudflare?* Cloudflare. Retrieved April 28, 2023, from https://www.cloudflare.com/learning/what-is-cloudflare/

Comissão Nacional de Proteção de Dados [CNPD]. (2021, April 27). *CENSOS 2021: CNPD SUSPENDE FLUXOS PARA OS EUA [2021 CENSUS: CNPD SUSPENDS FLOWS TO THE USA]*. [News]. Comissão Nacional de Proteção de Dados [National Data Protection Commission].

https://www.cnpd.pt/comunicacao-publica/noticias/censos-2021-cnpd-suspende-fluxos-para-os-eua/

Cory, N., & Dascoli, L. (2021, July 19). *How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address* Them. Information Technology & Innovation Foundation. Retrieved April 28, 2023, from https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost/

Cyberscoop, "Researchers ID new RAT developed by Chinese hacking group with growing target list," June 12, 2022.Retrieved April 28 from https://cyberscoop.com/chinese-hackers-pingpull-rat-espionage/

Daskal, J., & Sherman J. (2020, June). *Data Nationalism on the Rise: The Global Push for the State Control of Data*. Data Analyst. https://datacatalyst.org/wp-content/uploads/2020/06/Data-Nationalism-on-the-Rise.pdf

Department of Communications and Digital Technologies, Republic of South Africa. (2021, April 1). *Draft National Policy on Data and Cloud. Electronic Communications Act No. 306.* https://www.gov.za/sites/default/files/gcis_document/202104/44389gon206.pdf

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on Measures for a High Common Level of Cybersecurity Across the Union, Amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and Repealing Directive (EU) 2016/1148 (NIS 2 Directive), recital 121 (2022). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555&qid=1683666832600

Drake, W. (2018, January). *Data Localization and Barriers to Cross-Border Data Flows Towards a Multitrack Approach [White Paper].* World Economic Forum. *https://www3.weforum.org/docs/White_Paper_Data_Localization_Barriers_Cross-Border_Data_Flows_report_2018.pdf*

European Data Protection Board. (2022, December 19). *The Portuguese Supervisory Authority fines the Portuguese National Statistics Institute (INE) 4.3 million EUR*. [News]. https://edpb.europa.eu/news/national-news/2022/portuguese-supervisory-authority-fines-portuguese-national-statistics_en

European Data Protection Board. (2018). *Guidelines on derogations of Article 49 under Regulation 2016/679*. Retrieved April 30, 2023, from https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf

European Union Agency for Cybersecurity (ENISA). (2015, December). *Information sharing and common taxonomies between CSIRTs and Law Enforcemen*t. Retrieved April 30, 2023, from https://www.enisa.europa.eu/publications/information-sharing-and-common-taxonomies-between-csirts-and-law-enforcement

Fefer, R. (March 26, 2020). *Data Flows, Online Privacy, and Trade Policy.* Congressional Research Service, R45584. Retrieved April 30, 2023, from https://crsreports.congress.gov

GDPR-info.eu. (n.d.). *Consent under the GDPR.* Retrieved April 30, 2023, from https://gdpr-info.eu/issues/consent/#:~:text=The%20basic%20requirements%20for%20the,given%20on%20a%20voluntary%20basis

IBM. *What is cyber resilience?* (n.d.). Retrieved April 28, 2023, from https://www.ibm.com/topics/cyber-resilience

Interim Report of The Expert Group on Data Free Flow with Trust. (2022). Ministry of Economy, Trade and Industry of the Government of Japan. https://www.meti.go.jp/shingikai/mono_info_service/data_ekkyo_iten/pdf/20220228_2e.pdf

Johnson, C. S., Badger, M. L., Waltermire, D. A., Snyder, J., & Skorupka, C. (2016, October). *Guide to Cyber Threat Information Sharing* (NIST SP 800-150; p. NIST SP 800-150). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-150

Junck, R. D., Klein, B. A., Kumaki, A., Kumayama, K. D., Kwok, S., Levi, S. D., Talbot, J. S., Vermynck, E.-C., & Zhang, S. (2021, November 3). *China's New Data Security and Personal Information Protection Laws: What They Mean for Multinational Companies*. Skadden, Arps, Slate, Meagher & Flom LLP. https://www.skadden.com/insights/publications/2021/11/chinas-new-data-security-and-personal-information

Kennedy-Mayo, D., & Swire, P. (2021, April 29). *New urgency about data localization with Portuguese decision | Privacy Perspectives*. Retrieved April 28, 2023, from https://iapp.org/news/a/new-urgency-about-data-localization-with-portuguese-decision/

López González, J., F. Casalini and J. Porras (2022, June 13), "A Preliminary Mapping of Data Localisation Measures", *OECD Trade Policy Papers*, No. 262, OECD Publishing, Paris, https://doi.org/10.1787/c5ca3fed-en

Matheson, L. (March, 2023). *NOT-SO-STANDARD CLAUSES: Examining Three Regional Contractual Frameworks for International Data Transfers.* (Future of Privacy Forum (FPF). Retrieved April 30, 2023, from https://fpf.org/wp-content/uploads/2023/03/FPF-SCC-Not-So-Standard-Clauses-Report-FINAL-single-pages-1.pdf

Ministry of Health, Labour and Welfare of Japan. (2022, March). *Iryo joho shistem no anzenkanri ni kansuru gaidorain dai 5.2 han honpen [Guidelines for the Safety Management of Medical Information Systems Edition 5.2 Main Part].* Ministry of Health, Labour and Welfare of Japan. Retrieved April 29, 2023, from https://www.mhlw.go.jp/content/10808000/000936160.pdf

Morgan, Lewis & Bockius LLP. (2018, October). *The eData Guide to GDPR: Transfer of Data in the GDPR: The Definition of Legitimate Interest.* Retrieved April 30, 2023, from https://www.morganlewis.com/pubs/2018/10/the-edata-guide-to-gdpr-transfer-of-data-in-the-gdpr-the-definition-of-legitimate-interest

National Cybersecurity and Communications Integration Center. (2016, October). *Critical Infrastructure Threat Sharing Framework: A Reference Guide for the Critical Infrastructure Community Information.* Retrieved April 30, 2023, from https://www.cisa.gov/sites/default/files/publications/ci-threat-information-sharing-framework-508.pdf

National Cybersecurity and Communications Integration Center. (n.d.). *cyber resiliency—Glossary | CSRC*. Retrieved April 28, 2023, from https://csrc.nist.gov/glossary/term/cyber_resiliency

Palo Alto Networks. (2019). *National data security action plan: Cybersecurity strategy for Australia*. Retrieved April 30, 2023, from https://www.homeaffairs.gov.au/reports-and-pubs/files/national-data-security-action-plan/palo-alto-networks.pdf

Palo Alto Networks. (2022a, June 24). *RE: Call for Views on the National Data Security Action Plan*. Retrieved April 30, 2023, from https://www.homeaffairs.gov.au/reports-and-pubs/files/national-data-security-action-plan/palo-alto-networks.pdf

Palo Alto Networks. (2022b, March 10). *PingPull Gallium: Chinese APT10 Targets Russia and Mongolia in the Defense Sector*. Unit 42. Retrieved April 30, 2023, from https://unit42.paloaltonetworks.com/pingpull-gallium/

Personal Information Protection Commission of Japan. (n.d.). *Q4-31 Shinryo johou tou no kojin deta no hozon wo gaikoku no jigyosha ni itaku surukoto ha dekimasu ka? [Is it possible to outsource the storage of personal data, such as medical information, to a foreign entity?].* Retrieved April 29, 2023, from https://www.ppc.go.jp/all_faq_index/faq3-qb4-31/

Regulation (EU) 2016/679 of The European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), c. 5. (2016).
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

Republic of Philippines National Privacy Commission. (June 28, 2021). *Guidance For the Use of The Asian Model Contract Clauses And ASEAN Data Management Framework*. Retrieved April 30, 2023, from https://www.privacy.gov.ph/wp-content/uploads/2021/06/Advisory-ASEAN-MCC-DMF_FINAL-signed.pdf

Robinson, L., Kizawa, K., & Ronchi, E. (2021). *Interoperability of privacy and data protection frameworks*. Going Digital Toolkit Note, No. 21. Retrieved April 30, 2023, from http://goingdigital.oecd.org/data/notes/No21_ToolkitNote_PrivacyDataInteroperability.pdf

Roth, *Y.* (2021, March 24). *How Forcing TikTok To Completely Separate Its US Operations Could Actually Undermine National Security.* Techdirt.com. Retrieved April 28, 2023, from https://www.techdirt.com/2023/03/24/how-forcing-tiktok-to-completely-separate-its-us-operations-could-actually-undermine-national-security/.

Ryan, P., Falvey, S., & Merchant, R. (2013). *When the Cloud Goes Local: The Global Problem with Data Localization.* Computer, 46(12), 54-59. https://doi.org/10.1109/MC.2013.410

Swire, P., & Kennedy-Mayo, D. (2022, June 24), *The Effects of Data Localization on Cybersecurity.* Georgia Tech Scheller College of Business Research Paper No. 4030905, http://dx.doi.org/10.2139/ssrn.4030905.

United Nations Conference on Trade and Development (UNCTAD). (2016). *Data protection regulations and international data flows: Implications for trade and development.* Retrieved April 30, 2023, from https://unctad.org/system/files/official-document/dtlstict2016d1_en.pdf

Zibak, A., & Simpson, A. (2019), *Cyber Threat Information Sharing: Perceived Benefits and Barriers*. Association for Computing Machinery. https://doi.org/10.1145/3339252.3340528

Columbia SIPA Capstone Report

May 2023