Suleiman, Ajisatria

Research Report

A Study on the Access of Ministry, Government Agencies, and Law Enforcement Authority to Electronic System Organizers' Data and Systems

Policy Paper, No. 39

Provided in Cooperation with:
Center for Indonesian Policy Studies (CIPS), Jakarta

Suggested Citation: Suleiman, Ajisatria (2021) : A Study on the Access of Ministry, Government Agencies, and Law Enforcement Authority to Electronic System Organizers' Data and Systems, Policy Paper, No. 39, Center for Indonesian Policy Studies (CIPS), Jakarta

This Version is available at:
https://hdl.handle.net/10419/249419

CIPS
Center for Indonesian Policy Studies

idEA
Asosiasi E-Commerce Indonesia

Policy Paper No. 39

A Study on the Access of Ministry, Government Agencies, and Law Enforcement Authority to Electronic System Organizers' Data and Systems

by Ajisatria Suleiman

www.cips-indonesia.org

Policy Paper No. 39

A Study on the Access of Ministry, Government Agencies, and Law Enforcement Authority to Electronic System Organizers' Data and Systems

Author:
Ajisatria Suleiman
Center for Indonesian Policy Studies (CIPS)

Copy Editor:
Janet Bufton

Acknowledgement:
This paper is supported by the Indonesian E-Commerce Association (IdEA), who respect the independence of our analysis. To strictly safeguard our academic integrity and institutional non-partisanship, CIPS exclusively cooperates with donors who do not determine the findings, conclusions, or recommendations presented in CIPS publications.

Cover:
freepik.com/onlyyouqj

Jakarta, Indonesia
September, 2021

CONTENT

List of Tables

GLOSSARY

ESO:
Electronic Service Organizers.

MOCI:
Ministry of Communication and Informatics.

MOCI Regulation No. 5/2020:
Ministry of Communication and Informatics Regulation No. 5/2020 on Electronic Service Organizers in the Private Sector.

Dwang middelen:
Means of coercion.

SMPI:
Information Security Management Systems.

EXECUTIVE SUMMARY

The authority of government agencies to access the electronic data of platforms or private electronic system organizers (ESOs) has been a widely discussed topic among international experts due to its various practices across the world. Indonesia stipulates provisions on this issue through the Ministry of Communication and Informatics (MOCI) Regulation No. 5/2020 on Electronic System Organizers (ESOs) in the Private Sector. Reflecting from the opinions from international scholars and experiences of other countries this paper provides several recommendations to improve the substance of the regulation. From the legal aspect, a review and appeal mechanism by an independent board and a more robust legal basis are needed to ensure public's political participation. Furthermore, it is ideal that the Law on Personal Data Protection is signed and issued before the access authority by government agencies can work properly. In the current situation, MOCI should serve as a governing body and privacy safeguard to ensure that accesses by ministries and government agencies for supervision purposes are in accordance with the principles of personal data protection. This paper concludes that access to ESO's system might not be the best practice, and therefore should be taken as a last resort after all mitigation actions on information security have been carried out.

INTRODUCTION

The Ministry of Communication and Informatics (MOCI) Regulation No. 5/2020 on Electronic System Organizers (ESOs) in the Private Sector, that is set to come into effect in mid-May 2021, brings a significant change to the governance of access to ESOs' data and systems. Article 21 of the regulation states that private ESOs are required to provide access to their Electronic Systems and/or Electronic Data to (a) ministries or government agencies for supervision purposes in accordance with laws and regulations, and (b) law enforcement authorities for law enforcement purposes in accordance with laws and regulations.

Article 3 (4) point (i) obliges all private ESOs to register and provide a statement letter guaranteeing access to their systems and data, for law enforcement and supervision purposes in accordance with the relevant laws and regulations.

On the one hand, provisions on the governance of access to data and system in the MOCI Regulation No. 5/2020 can serve as the guidelines and standard reference for the ministries/ government agencies and law enforcement authorities to exercise their authority and request for access to ESOs' data and systems. In this case, MOCI can play a role as a governing and advisory body to ensure that ministries and law enforcement authorities can exercise their power with careful consideration to personal data protection and due process of law.

> If it is not exercised carefully, access to systems can potentially cause a security lapse that disrupts the ESOs' information security system posture.

On the other hand, access to ESOs' data and systems is a sensitive issue because it is related to means of coercion (*dwang middelen*) that might potentially infringe human rights protection and individual freedom. It also has a strong correlation with the protection of personal data and trade secrets (including relevant intellectual property rights such as copyrights). If it is not exercised carefully, access to systems can potentially cause a security lapse that disrupts the ESOs' information security system posture. These issues are public interest and should be protected.

The MOCI Regulation No.5/2020 essentially addresses these fundamental issues. For example, regarding access to data, the regulation requires an assessment on its significance, proportionality, and legality. Additionally, the scope and type of system or electronic data that will be accessed must be explicitly stated. The access can be used only for purposes stated in the request. In terms of access authorization, Article 30 stipulates that there are several components that must be protected, such as the integrity, availability, and confidentiality of the Electronic Data; reliability and security of the Electronic System and related Personal Data.

Nevertheless, further in-depth analysis is needed to assess whether the MOCI Regulation No. 5/2020 has accommodated various key elements to safeguard the general principles of human rights, intellectual property rights, and personal data protection.

Discussions surrounding this topic are not unique to Indonesia, considering that similar debates can also be seen in other countries. In the United States, for example, debates have been going around the definition of "meta-data" and "data", where the access to meta-data only requires a

subpoena, whereas access to data requires a court order (Nissenbaum et al., n.d.). There are also debates relating to national security interests, in which data authorization access can be given with simpler procedures when it pertains to security threats, such as terrorism (Rubinstein et al., 2014).

Amidst these debates, experiences from other countries can be used as references to assess the lawfulness and fairness of the MOCI Regulation No. 5/2020. Countries such as the United States, Brazil, South Korea, China, and India have their own regulations concerning government access to data. With the exception of the Golden Shield project in China, these countries have specific legislations that are discussed through a political process in the parliament, which represents the public's voice in the policymaking process. References and literature from these countries further suggest that government access is generally used in electronic data rather than electronic systems.

Based on this background, the paper attempts to answer these questions:

a. What are the general principles that should be used as the guidelines to access the data and systems of digital business actors?
b. Has the MOCI Regulation No. 5/2020 adopted the existing general principles on data access?
c. What can be learned from the practices of data governance in other countries?
d. How could the business actors respond to the current debates on data governance?
e. What policies does Indonesia need in the future with regards to data governance?

THE GENERAL PRINCIPLES AND PUBLIC INTEREST

> Technology companies have the right and obligation to carefully assess whether the government request is legitimate and whether it complies with the international human rights standards.

The lawfulness of a government agency to access the data of platforms or private ESOs have been extensively discussed by experts. The implementation guidelines from the Global Network Initiative (GNI)[1] mentions that it is not sufficient for a technology company to say, "we are just playing by the rules" (Global Network Initiative, 2018). Technology companies have the right and obligation to carefully assess whether the government request is legitimate and whether it complies with the international human rights standards. GNI's guidelines also state that, should a company be asked to provide information to a government agency, it has the right and obligation to:

1. Narrowly interpret and implement government demands that appear to be violating personal data protection.
2. Seek clarification or modification from the authorized officials of demands that appear overbroad, unlawful, and inconsistent with the prevailing laws and international human rights standards on privacy.
3. Request a clear communication, preferably written, that explains the legal basis of the government demands for personal information, including the name of the requesting government agency, as well as the name, title, and signature of the authorized official.
4. Require the government to adhere to the established domestic legal procedure in accessing personal data.
5. Adopt policies and procedures to respond to instances where the government fails to adhere to the established legal procedures. Such policies and procedures should include the consideration of the rationale behind the objection of the government demands.
6. Narrowly interpret the government authority to access personal data.
7. Challenge the government in domestic courts or seek assistance from relevant authorities, international human rights bodies, or non-governmental organizations when faced with government demands that appear inconsistent with domestic laws or procedures or the international human rights standards on personal data protection (Global Network Initiative, 2018, pp. 8–9).

[1] The Global Network Initiative is a multi-stakeholder collaboration of companies, human rights activists, investors, and other stakeholders that ensures that technology companies comply to human rights principles, personal data protection, and freedom of expression, especially related to access to data and content blocking. See https://www.globalnetworkinitiative.org/.

Nico van Eijk, professor of Media and Telecommunications Law and the Director of the Institute for Information Law (IViR, Faculty of Law, University of Amsterdam) identified seven general principles to ensure the oversight and check-and-balances over access to data by the government as follows (van Eijk, 2017):

1. Oversight should be comprehensive in three respects: (a) the government (executive branch), legislative, judiciary, and specialized commission should all play a role in the supervisory process, (b) Supervision should be done prior, ongoing, and after the fact has been obtained, and (c) the mandate of the oversight bodies should include the review on the lawfulness and effectiveness of the access request.
2. The supervision should include all stages of the data cycle, namely data collection, storage, querying, and analysis.
3. The oversight bodies should be independent from intelligence agencies and the government, similar to independent judicial mechanisms.
4. The oversight can be conducted before the implementation of the access (prior oversight) or the combination of prior and after-the-fact oversight by an independent specialized commission; there is an oversight function by a parliamentary committee; and possibility for individuals to complain before an independent body.
5. The oversight bodies should be able to declare the actions unlawful and provide for redress.
6. The oversight should ensure an opportunity for the reporting and reported parties to rebut each other (adversarial).
7. The oversight bodies should have sufficient resources to work effectively.

Other prominent scholars, Jennifer Daskal, professor and the Director of the Tech, Law, Security Program from the American University Washington College of Law, and Andrew K. Woods from the University of Arizona College of Law proposed several general principles to ensure the equality of legal protection of access to data (Daskal & Woods, 2015). These principles can be used as guidelines as follows:

1. **Independent authorization**. An independent body is needed to ensure that an access request is based on an appropriate cause, in accordance with the agency's authority based on the existing laws and regulations, and proportional. Such an independent body is usually a judiciary body, which issues a court order. The existence of a judiciary body can also facilitate complaints or objections in the case of the ESO or individuals objecting to the access request.
2. **A cause**. There is a strong rationale or factual basis for the access request, such as a crime or to supervise a certain activity. This principle prevents the abuse of power of the party who requests for access for purposes beyond their authority.
3. **Particularity**. The access request should specifically refer to a particular individual, account, or device, and describe the type, time frame, and data sought. This principle also prevents the abuse of power of the party who requests for access for purposes beyond their authority.
4. **Legality**. All access requests should have a legal basis in the relevant laws and regulations. The legal consideration should be explicitly mentioned in every request.

5. **Proportionality**. Every country should define what actions can prompt an access request. For example, for law enforcement purposes, only criminal acts with certain threats can prompt the right to access personal data.
6. **Notice to the users/owners or data subjects**. In line with the principles of personal data protection, data subjects should be notified with regards to the access request. In certain cases, such as in a criminal investigation process, the notification can be delayed until the investigation reaches a particular stage. However, the party who requests for the access to data still has the obligation to notify the data subjects.
7. **Guarantee of freedom of expression**. An access request to data or systems should not be used as an instrument to repress citizens who wish to exercise their rights to freedom of expression and opinion.
8. **Data collection minimization**. Personal data collection should be limited only to personal data related to the cause.
9. **Exception in emergency situations**. Daskal and Woods (2015) also realized that the process and procedure of access requests can be excluded or simplified in an emergency situation. Hence, a regulation should categorize what constitutes an emergency, such as a situation that potentially jeopardizes one's safety or life (life-threatening situation).
10. **Transparency**. Ministries, government agencies, or law enforcement authorities are required to uphold transparency in requesting for data access. There should be a mechanism to show the number of access requests, including their types, scopes, and other relevant information, such as a periodic annual report from the law enforcement authorities or ministries/government agencies, or other forms of audit.

THE SUBSTANCE OF THE MOCI REGULATION NO. 5/2020 AND ITS ISSUES

The MOCI Regulation No. 5/2020 regulates two (2) subjects and two (2) material objects.

From the perspective of the subject, the MOCI Regulation No.5/2020 gives authorization to ministries/government agencies (defined as *the State Administration Agencies responsible to supervise and issue regulations in their sectors*), and law enforcement authorities.

From the perspective of the object accessed, the MOCI Regulation No.5/2020 contains provisions on the access to "electronic data" and "electronic system". The regulation explains that "Electronic Data" are "data in electronic form which is not limited to text, sound, image, map, design, photo, electronic data interchange (EDI), electronic mail, telegram, telex, telecopy or the like, letter, sign, number, access code, symbol, or perforation". Meanwhile, "Electronic System" is "series of electronic procedures and devices that serve to prepare, collect, process, analyze, store, display, announce, send, and/or disseminate Electronic Information.". The difference between the risks of access to data and systems are explained in the previous chapter.

With that as a basis, the comparison matrix of the two subjects and objects of the regulation below was developed to allow a more in-depth analysis:

Table 1.
Comparison Matrix of The Two Subjects and Objects of The MOCI Regulation No. 5/2020

	Ministries/Government Agencies	Law Enforcement Authorities
Data	**Requirements to submit** a. The legal basis of authority of the requesting Ministry or Government Agencies; b. The objectives, targets, and purposes of the request; and c. A specific description of the type of the requested Electronic Data **Deadline**: Five days **Methods**: Link or other methods, within a certain period of time	**Requirements to submit** a. The legal basis of authority of the requesting Law Enforcement Authorities; b. The objectives, targets, and purposes of the request; c. A specific description of the requested Electronic Data; d. The criminal offense that is being investigated, prosecuted, or tried; and e. Additional requirements for communication contents: ***letter of determination from the head of the district court in the area where the Law Enforcement Institution has authority.*** **Scope:** criminal acts in which the criminal punishment is in the form of imprisonment for a minimum of 2 (two) years, and data related to Indonesian citizens or legal bodies **Deadline:** Five days **Methods:** Link or other methods, within a certain period of time
System	**Requirements to submit** a. The legal basis of authority of the requesting Ministry or Government Agencies;	**Requirements to submit** a. The legal basis of authority of the requesting Ministry or Government Agencies;

	b. The objectives, targets, and purposes of the request; and c. A specific description of the type of the requested Electronic Data, and d. The officials from the Ministry or Government Agency that will access the requested Electronic System **Deadline:** Five days **Methods:** Submission of the inspection or audit results of the Electronic System whose scope is requested by the Ministry or Government Agency	b. The objectives, targets, and purposes of the request; and c. A specific description of the type of the requested Electronic Data; d. The criminal offense that is being investigated, prosecuted, or tried; e. The law enforcer officers that will access the requested Electronic System; and f. ***letter of determination from the head of the district court in the area where the Law Enforcement Institution has authority***. **Scope**: criminal acts in which the criminal punishment is in the form of imprisonment for a minimum of 2 (two) years, and data related to Indonesian citizens or legal bodies **Deadline**: Five days **Methods**: Submission of the inspection or audit results of the Electronic System whose scope is requested by the Ministry or Government Agency

Source: MOCI Regulation No.5/2020, processed by Author

From the comparison above, issues found in MOCI Regulation No.5/2020 will be discussed below:

Access to data *vis-à-vis* confiscation. Access to data can be compared to the electronic confiscation of an item. With this analogy, regulations regarding confiscation in Article 1 point 16, Article 38 to 46, Article 82(1) and (3) in the context of a pre-trial review, Article 128 to 130, Article 194, and Article 215 of the Indonesian Criminal Procedure Code ("KUHAP") will be discussed further. Confiscation is defined under Article 1 point 16 of the Criminal Procedure Code as: "*a set of actions done by an investigator to seize or store movable or immovable, tangible or intangible assets into their possession for the purpose of authentication in an investigation, prosecution, and trial*".

Because confiscation is a means of coercion (*dwang middelen*) that might violate human rights, Article 38 of the Indonesian Criminal Procedure Code stipulates that confiscation can be carried out only by an investigator with an approval from a local district court. However, during an emergency, the confiscations can take place first, and the investigator has the obligation to report it afterwards to the head of the district court to obtain his approval.

The internal regulation of the Indonesian National Police stipulates that a confiscation can be carried out without an approval letter or warrant from the head of a district court, but this only applies to movable assets. For cases of apprehension *in flagrante delicto*, an approval/special approval letter and confiscations warrant from the chairman of a district court are also not required. However, the confiscations can be carried out only for items and equipment that are allegedly used in criminal offences or other items that serve as a proof.

With this comparison, the difference between access to system vis-à-vis confiscation can be seen. The MOCI Regulation No. 5/2020 divides data into two types: those that require a letter of determination from the district court and those that do not. For communication contents in particular, a letter of determination from the district court is required. Meanwhile, the Indonesian Criminal Procedure Code regulated that the exception of court is determined from its element of urgency, rather than the type of confiscated assets. The provisions in the Criminal Procedure Code are considered more in line with human rights principles compared to those of the MOCI Regulation No. 5/2020.

“With this comparison, the difference between access to system vis-à-vis confiscation can be seen. The MOCI Regulation No. 5/2020 divides data into two types: those that require a letter of determination from the district court and those that do not. For communication contents in particular, a letter of determination from the district court is required. Meanwhile, the Indonesian Criminal Procedure Code regulated that the exception of court is determined from its element of urgency, rather than the type of confiscated assets. The provisions in the Criminal Procedure Code are considered more in line with human rights principles compared to those of the MOCI Regulation No. 5/2020.”

Access to system *vis-à-vis* search. Access to systems can be compared to a search, but in this context, the law enforcer authority enters the “office/house” of the ESOs. The office/house is the electronic system of the ESOs. With this analogy, the regulation concerning confiscations in Article 33 of the Indonesian Criminal Procedure Code, which states that a warrant from the head of the local district court can prompt a search as required, can be further studied. In addition, two witnesses must be present in each instance of entry to a house, if the suspect or owner has given their consent, and must be witnessed by the village head or head of the neighborhood, if the suspect or owner has refused or is not present. In principle, a search can be carried out with a warrant from the head of the local district court. This requirement aims to ensure the protection of human rights over their house. It also prevents the search from being carried out by the investigator without limitation and supervision.

Moreover, Article 34 of the Indonesian Criminal Procedure Code stipulates about a search in an urgent situation, stating that “*in urgent and compelling circumstances, where an investigator must act immediately and cannot possibly first ask for a warrant, without detracting from the provision of Article 33 (5), the investigator can carry out a search in limited areas. In this case, the investigator shall not be allowed to examine or seize letters, books, and other documents which are not related with the offense concerned or are presumed to have been used in committing said offense and for which purpose he shall be obliged to report immediately to the chairman of the local district court to obtain his approval*”.

The explanation in Article 34 (1) of the Indonesian Criminal Procedure Code states that “urgent” and compelling circumstances are instances where the searched place is suspected to be occupied by a suspected or accused criminal who might escape or repeat an offense, or there might be destruction or transfer of suspected items, and a warrant from the district court is not possible to be obtained properly and in a timely manner.

With this analogy, we can see the difference between access to system *vis-à-vis* search. Access to systems by ministries/government agencies does not require a decision from the district court. This is different from the Indonesian Criminal Procedure Code that requires a decision from the court to guarantee human rights, with the exception of certain urgent situations.

"With this analogy, we can see the difference between access to system vis-à-vis search. Access to systems by ministries/government agencies does not require a decision from the district court. This is different from the Indonesian Criminal Procedure Code that requires a decision from the court to guarantee human rights, with the exception of certain urgent situations."

Access to systems. Discussions about access to electronic systems are uncommon, both in theoretical debates and its practices in other countries. Access to systems is an unconventional practice due to its high information security risks that might disrupt the users of the system, including the public (Rubinstein et al., 2014).

The MOCI Regulation No. 5/2020 does not clearly delineate the objectives of access to systems and in what way access to electronic systems is necessary. If the final objective is to gain access to data, access to electronic systems shall be taken as a final resort when the government has failed to obtain the accessed data.

Although similar, access to data and access to systems have different implications. Access to systems poses high information security risks, especially if it is not accompanied with an access control and appropriate operational security measures (OECD, 2019). The ISO/SNI 27001 Standard of Information Security Management Systems (SMPI), as adopted by the National Cyber and Crypto Agency, regulates the access control and operational security to ensure that access to electronic systems is carried out in accordance with the universal principles of the SMPI. Below are several points in the Standard that are relevant to access to system:

Table 2.
Points in The Information Security Management System (SMPI) Which are Related to The Access to System

Annex A9: *Access Control*	The accessing party can only access the network or network services when they have a specific authorization. The access should be controlled through a secure and limited login procedure in accordance with the access control policy.
Indicator	1. There is a multi-factor authentication 2. There are unique credentials 3. There are verification and authentication mechanisms 4. Shared login restriction 5. Network access setting based on job-role, where the admin system can change the access rights both temporarily and permanently 6. There is an end of session or automatic log-off/log-out after a certain period of time.

Annex A12: ***operations security***	The availability of an event log to record the activities of the users, including exclusions, errors, and other security incidents to be recorded and analyzed periodically.
Indicator	1. Attribution of session duration and actions within the network of specific users 2. There is a supervision of the network 3. There is a supervision of the activities in the files or folders, including copying, moving, and deleting 4. There is a periodical security report and audit.

Source: ISO/SNI 27001 standard on Information Security Management System (SMPI).

The standards in Annex A9 and A12 show that access to systems has high security risks. There is a probability of unauthorized access, which can happen due to a hacking, identity fraud, or shared login practice between the personnel within the ministries or agencies (OECD, 2019). Such an incident significantly increases the security risks for ESOs. Moreover, from the operational viewpoint, there are also several actions that undermine the security, such as copying or deleting files and folders, both intentionally and unintentionally.

Hence, in addition to complying with the general principles of granting access, both ESO's system and authorities from ministries/government agencies who access the system should adhere to the principles of information security, at least those stipulated in the ISO/SNI 27001 Standard. In practical terms, the consequences should be further studied, such as through an initial audit of the law enforcement authorities or ministries/ government agencies who wish to access the system of an ESO, that is to ensure that the system and the access per se do not conflict with the best practices of information security.

"Hence, in addition to complying with the general principles of granting access, both ESO's system and authorities from ministries/government agencies who access the system should adhere to the principles of information security, at least those stipulated in the ISO/SNI 27001 Standard. In practical terms, the consequences should be further studied, such as through an initial audit of the law enforcement authorities or ministries/government agencies who wish to access the system of an ESO, that is to ensure that the system and the access per se do not conflict with the best practices of information security."

Access by law enforcement authorities vs. access by ministries or government agencies. Unlike the provisions on access to data/ system by law enforcement authorities that have comparisons from the Indonesian Criminal Procedure Code, access to data/ system by ministries or government agencies do not have uniform guidelines. Moreover, in international best practices, except for financial, taxation, and state intelligence/security sectors, government agencies are rarely given the authority to access data or systems of ESOs (OECD, 2019). The provisions on access by ministries or government agencies in the MOCI Regulation No. 5/2020 are actually based on Government Regulation (GR) No. 71 of 2019 on Implementation of Electronic Systems and Transaction.

Article 21 of GR 71 states that "Private Electronic System Organizers shall give access to Electronic System and Data for supervision and law enforcement purposes in accordance with laws and regulations". In this context, it means that the ministries or government agencies' needs for data or systems are a part of the supervision of the relevant ESO. However, Article 35 of GR 71 states that "provisions on the supervision of Electronic System in certain sectors **shall be made**

by relevant Ministries or Government Agencies *following a coordination with the Minister*". When the provisions regarding supervision are formulated by each ministry or government agency, the existence of articles on access to data and/or system by ministries/government agencies under the MOCI Regulation No.5/2020 can be legally debated. Considering this, there is actually no delegation of authority from GR 71 to the MOCI to further regulate access to data or systems by ministries or government agencies.

The approach in Article 35 of GR 71 that leaves the matter to each ministry or government agency is seen as in line with the current practices in Indonesia or overseas, in which access by a ministry or government agency is usually based on the authority embedded to the Laws (the formulation of which has undergone a political process through the representatives in the House of Representatives), to accommodate public participation. Regarding this, sectors that generally need access to data are taxation, financial, and state security or intelligence sectors. In Indonesia, these sectors already have a robust legal basis equivalent to a Law that becomes the basis for data collection for each sector's purposes. For example:

- *Directorate General of Taxes,* for tax audit. This authority is in accordance with Law No. 6/1983 on General Provisions and Tax Procedures as amended several times, most recently by the Job Creation Act.
- *Financial Services Authority (OJK) and Bank Indonesia*, either for licensing supervision/ inspection or financial system supervision purposes in order to assess systemic risks and conduct an inspection to such risks. This authority is in line with the Laws on Bank Indonesia and Financial Services Authority, as well as relevant Bank Indonesia Regulations (PBI) and Financial Services Authority Regulations (POJK).
- *State Intelligence Agency*, for activities that threaten national interests and security, which are related to ideology, economy, social, culture, defense and security, and other public sectors, such as food, energy, natural resource, and environment; and/or terrorism, separatism, espionage, and sabotage activities that jeopardize the national safety, security, and sovereignty, including those undergoing a legal process based on the Law No. 17/2011 on State Intelligence.

Beyond these three sectors, Indonesia has a precedence in the online transportation sector to give the government access to data in the form of digital dashboards. Under the Minister of Transportation Regulation No. 118/2018 concerning the Implementation of Special Rental Transportation, transportation application companies have the obligation to develop and provide access to their digital dashboards that contain:

a. the name of the company, person in charge, and address of the Application Company;
b. data of all Special Rental Transportation company partners;
c. data of all vehicles and drivers;
d. service operational monitoring access in the form of order transaction data through the application, including the origins and destinations of the trips and the tariffs; and,
e. customer service in the forms of the Application Company's telephone and electronic mails.

The provisions of data access through digital dashboards in the Minister of Transportation Regulation No. 118/2018 are sufficiently detailed and equivalent to a tax audit or inspection in the financial sector. Moreover, the requested data are linked to the identity of the drivers and order transactions, which are related to various personal data protection and data that are considered trade secrets. If not managed well, such data might be potentially misused for an unhealthy business competition, such as to see the competitors' penetration in different regions across Indonesia. The problem is that provisions on digital dashboards are not based on an explicit legal basis in Law No. 22/2009 on Road Traffic and Transportation. The MOTr Regulation No. 118/2018 does not even refer to this Law.

Other than the three general sectors and one special sector of transportation application in Indonesia, access requests to data by ministries or government agencies are generally related to license inspection. Ministries or government agencies can request for additional documents or conduct a field inspection to ensure the compliance of a business license.

With a wide array of access typologies by ministries/government agencies for supervision purposes, in order to ensure that the current practices work well and to prevent multi-interpretation of authority, as well as to adhere to the spirit of Article 35 of GR 71, the Ministry of Communication and Informatics in general, and the MOCI Regulation No. 5/2020 in particular, should be treated as the instruments that advise and ensure that every access request from ministries/government agencies is in line with the principles of personal data protection, in addition to the specific provisions in the respective sector.

> "The Ministry of Communication and Informatics in general, and the MOCI Regulation No. 5/2020 in particular, should be treated as the instruments that advise and ensure that every access request from ministries/government agencies is in line with the principles of personal data protection, in addition to the specific provisions in the respective sector."

When the MOCI and the MOCI Regulation No. 5/2020 are placed as the instruments of advisory and harmonization, the MOCI Regulation No. 5/2020 should not create a new legal norm. Rather, it should be used as a technical guide to regulate the relationship and coordination between the agencies, such as, *first*, the relationship between the MOCI and law enforcement authorities. In this case, the MOCI can act as a privacy safeguard to ensure secure access from the law enforcement authorities. *Second*, the relationship between the MOCI and supervising ministries/government agencies. In this case, the MOCI can also act as a privacy safeguard and accordingly standardize the procedures of access rights of the institutions that are given such an authority based on the prevailing sectoral Law. *Third*, the relationship between the MOCI and civil servant investigators (PPNS). Civil servant investigators have a unique position because they work based on the sectoral Law, but still maintain coordination with the police. With a similar structure, the MOCI can become a coordination axis for the civil servant investigators to access data and electronic systems.

> "When the MOCI and the MOCI Regulation No. 5/2020 are placed as the instruments of advisory and harmonization, the MOCI Regulation No. 5/2020 should not create a new legal norm."

Review of the substance and formality of the access request. Even if a complete set of regulations on access rights to data or systems can be developed, there will be many debates and interpretations regarding the authorization access of the ministries, government agencies, or law enforcement authorities. This is normal, considering that electronic data or systems are the biggest assets of an ESO which has a complex dimension of confidentiality and intellectual property (Accenture, 2016). If we compare access to data and system to a confiscation and search, in order to support due process and checks and balances, every right to access needs to be complemented with a mechanism to file an objection or complaint as is with a pre-trial review in the Indonesian Criminal Procedure Code. Based on Article 77 point (a) of the Indonesian Criminal Procedure Code, a pre-trial review is the authority of the district court to examine and decide the legality or illegality of an arrest, detention, termination of investigation, or termination of prosecution. The Constitutional Court has given an additional authority to the pre-trial review in the Constitutional Decree No. 21/PUU-XII/2014, so that it has the authority to examine and decide the legality or illegality of an arrest, search, or seizure.

The MOCI Regulation No. 5/2020, in this case, does not include an appeal mechanism to review whether:

a. The basis of authority of ministries/government agencies or law enforcement authorities is appropriate.
b. The objectives, targets, and purposes of the ministries/government agencies or law enforcement authorities are appropriate.
c. The type of requested access is relevant with the basis of authority, objectives, and targets.

SEVERAL EXAMPLES OF COMPARISON IN OTHER COUNTRIES AND THE ROLES OF BUSINESS ACTORS

Stored Communication Act (SCA), Personal Data Protection, and The Case of Microsoft

In the United States, the protection of the right to privacy is stipulated in the fourth Amendment of the United States' Constitution, and further regulated under the Electronic Communications Privacy Act (ECPA) (Department of Justice, n.d.). The amendment of ECPA in 1986 introduced a new regulation concerning the Stored Communication Act (SCA) that functions as a *lex specialis*. The SCA limits the government actions to access data related to the users' information. For all inspection cases, including civil and state administrative lawsuits, the government agencies require a subpoena from the court to obtain information about the users' registration and IP address data (Schwartz Hannum PC, 2015). A subpoena is a request that can be submitted by anyone (individual, private entity, or government agency) to gain access to the opposing party's information.

Meanwhile, for criminal offenses in particular, a court document that is more substantial than a subpoena is required (Turner, 2016). The SCA states that, in order to obtain non-content data, a court-issued order is required. Non-content information includes the destination address, sender, CC/BCC, or timestamp of an electronic mail. For content information of an electronic mail, a search warrant is required, which needs a greater burden of proof from the investigator or prosecutor in the form of a "probable cause", that is to prove the justification for the requested content.

For example, Google explicitly states their compliance to the ECPA and SCA on their information request page (Google, n.d.). On a similar page, Facebook also wrote a similar statement (Facebook, n.d.):

> *"We disclose account records solely in accordance with our terms of service and applicable law, including the United States Federal Stored Communications Act ("SCA"), 18 USC sections 2701-2712. Under US law:*
>
> - *A valid subpoena issued in connection with an official criminal investigation is required to compel the disclosure of basic subscriber records (defined in 18 USC section 2703(c)(2)), which may include: name, length of service, credit card information, email address(es) and a recent login/logout IP address(es), if available.*
> - *A court order issued under 18 USC section 2703(d) is required to compel the disclosure of certain records or other information pertaining to the account, not including contents of communications, which may include message headers and IP addresses, in addition to the basic subscriber records identified above.*

- *A search warrant issued under the procedures described in the United States Federal Rules of Criminal Procedure or equivalent local warrant procedures upon presentation of a probable cause is required to compel the disclosure of the stored contents of any account, which may include messages, photos, videos, Timeline posts and location information."*

From the practice in the United States, we can understand that every access request requires an approval/stipulation from the court, except that the burden of proof for certain information is considered less substantial, requiring a subpoena and, in some cases, a search warrant to scrutinize whether there is a probable cause.

It should be noted that the SCA does not differentiate between access by law enforcement authorities and access by ministries or government agencies. This is because every inspection or supervision purpose from ministries or government agencies is administered through a legal avenue, be it in the context of civil, administrative, or criminal courts. This is different from the legal system in Indonesia, which allows for a legal investigation without a court proceeding, even though it is possible for the objecting party to file a civil or administrative lawsuit in the event of them objecting to the investigation process.

Despite having detailed stipulations on access to data, the SCA is still deemed incomplete, particularly in the aspect of personal data protection. The SCA does not regulate the obligation to give notice to the users when a technology company receives a request from law enforcement authorities.

One case that is quite interesting is the case of Microsoft Corporation v. US (2016), in which Microsoft filed for a court ruling to the United States District Court in Seattle, Washington (Columbia University Global Freedom of Expression, 2016). The object of dispute is the SCA of 1986, with Microsoft stating that the secrecy order from the Department of Justice (DoJ) had prevented them from providing their users with the search warrant from the public prosecutor of the DoJ. According to Microsoft, the secrecy order is against their obligation to protect their users' privacy. This case started in April 2016, and Microsoft in their lawsuit was supported by companies alike, such as Amazon, Apple, Google, Dropbox, and Salesforce. In October 2017, Microsoft revoked this lawsuit after the DoJ decided to change their policy regarding notification to the users or personal data subjects. Despite no amendments in the laws, the new policy of the Department of Justice "changes the regulation concerning data requests related to notification to the Internet users about the government agencies that access their information" and mandates a time restriction if a secrecy order needs to be issued.

In the efforts to file an appeal against the regulations in the SCA, Microsoft believes that provisions in the SCA have yet to accommodate the business needs. To ensure that trust is still maintained between a technology company and its users, Microsoft proposed three additional principles to be used as a reference.

First, transparency, where the users have the rights to know when the government requests for access rights to their records or e-mail communication contents. *Second*, digital neutrality. Only because data is in an electronic form or stored on cloud, does not mean that the protection is weaker. The principles of legal protection should still be applicable regardless of the type of

technology used. *Third*, justification. Although there is a justification to classify the access from the users, it should be adjusted to the needs of purposes of the running investigation case. If the government is not able to give an appropriate justification, the company like Microsoft has the obligation to notify about the access to their users (Smith, 2016).

Since Microsoft's lawsuit, the public prosecutors from the DoJ have changed their practices to comply with the general principles of personal data protection.

Examples of Practices in Other Countries

The experiences of other countries across the world show that government access to electronic data is common. However, these examples show that there are similarities in the approach used, in that access to data is always based on a legislation equivalent to a Law.

In **South Korea**, for example, government access to data can be found in various laws and regulations, especially in the Act on Personal Information Protection of Public Agencies (APIPPA), which was amended and combined with the Personal Information Protection Act (PIPA) and Telecommunications Business Act (TBA) in 2011. Besides PIPA and TBA, they also have other laws, including the Credit Information Act, Communication Privacy Act, the Real Name Finance Act, and Act on Use and Protection of DNA Identification Information (DNA Identification Act), which regulate data seizure through court orders or other means. In relation to transactional data, the Communication Privacy Act requires law enforcement authorities to give the subject a written notice within 30 days after obtaining records for investigation purposes (Jong, 2017).

The TBA contains details about data that are provided by telecommunication providers to fulfill the communication data request from the court, attorney, or the head of intelligence agency to be used in trials, criminal investigations, or for other national security purposes. Such data include the users' name, phone number, identification code used to identify the legitimate users of the communication network, and the beginning and end dates of subscription. In relation to anti-terrorism, to have access to contents on communication, trip information, and financial information, the National Intelligence Agency of South Korea can submit a request to Internet Service Providers (ISP) for contact, location, and other relevant personal information about an alleged terrorist without a court order.

One of the examples of access to data for a regulator supervision purpose is the access to personal information about copyright violators for the Ministry of Culture, Sports, and Tourism. To protect copyrights, South Korea's Copyright Act grants the minister the authority to demand ISPs to remove or stop the transmission of illegal reproductions or suspend the violator's account from online services for a limited period of time. Furthermore, based on the request from the copyright holder to collect data for prosecution, the minister can ask for the ISP to provide the list of people who allegedly possess copies or send illegal reproductions.

In India, provisions on access to data for law enforcement purposes can be found in Section 91 of the Code of Criminal Procedure, 1973 (CrPc) (Abraham, 2017). In addition, under the Reserve Bank Act, in order for the government to be able to access financial documents, they must request for an access to the Central Bank of India or obtain a court order and ask for an access

to the bank's branch office directly. To secure the access, the provisions of the Bankers Book Evidence Act apply to all information or documents stored by the system provider. The Securities and Exchange Board of India or SEBI also has wide access to the data of the private sector and is given the same authority as the court, including the obligation to open a new account and other documents.

The Information Technology Act (ITA) of 2008 gives the authority to the state security agency to access the information of users held by the private sector for investigation purposes (Abraham, 2017). In the "Data Protection" and "Reasonable Security Practices and Procedures and Sensitive Personal Data or Information" section, government access is widely allowed, meaning that (a) the security agency has no obligation to obtain an authorization prior to accessing the information; (b) the security agency is allowed to access the information of any government agencies; (c) the security agency is allowed to access all types of "sensitive data or personal information", and (d) the regulation allows the data to be used for general and public purposes.

In 2014, **Brazil** issued the *Marco Civil da Internet* to regulate Internet use (Magrani, 2017). This law serves as a regulation on law enforcer authority access to personal data, communication contents, users' identity information (IP addresses), and registration data from telecommunication and online providers. Regarding its confidentiality, financial data can only be obtained using a court order when it is needed for criminal investigation purposes. This law allows the Brazil Revenue Service (BRS) to request and obtain financial data directly from the financial agency without a judicial authorization.

In his paper, Magrani (2017) created a typology of authorizations required to gain access to data:

Table 3.
Typology of Authorizations Required to Gain Access to Data.

The Type of Data/ Authorization Required to Access The Data	Does The Access Require A Permit from The Court?	Is A Request for Data from The Police and The Prosecutor Office Sufficient?	The Regulatory Body Can Access the Data Only to Supervise The Activities That They Regulate
Communication Content	Yes	No	No
Communication Metadata	Yes	No	No
Registration Data	No	Yes	Yes
Non-communication; Transaction or Business Records	Yes	Unclear	Yes

Source: Magrani (2017).

In China, the State Security Law of 1993 grants the state security organization the authority to access any information or data held by anyone in China (Wang, 2017). Article 28 of the Law on Guarding State Secrets (2010 Revision) also states that "Operators and service providers of the Internet or any other public information network shall cooperate with the public security organization, the national security organization, and prosecutorial organization in the investigation of secret data leakage cases" (Wang, 2017).

One of the biggest projects in China is the Golden Shield project, which is led by the Ministry of Public Security (MPS) and other 11 agencies, including the State Taxation Administration, General Administration of Customs, Central Bank (PBOC), Ministry of Industry and Information Technology (MIIT), and other agencies. These agencies become a part of the initiative to develop an e-government system. This project and database refer to a framework set by the "Guiding Opinion on Construction of E-Government in our Country issued by the State Informatisation Leading Group". One of the databases for the Golden Shield project is the Basic Internet Database, which comprises data that have been collected monthly since 2006 from ISPs (Internet Service Providers), ICPs (Internet Content Providers), IDCs (Internet Data Centers), and e-mail services. There is no explicit authority given by any laws to build this database, and there are only order letters from local police authorities that ask for businesses to submit monthly reports with a data collection template created by the MPS. The collected data include all users' accounts and registration information, both individuals and companies, and other data sought by the government.

POLICY RECOMMENDATIONS

Based on the discussions regarding legal and public policy aspects in this paper, it can be concluded that provisions on access to data/system as regulated under the MOCI Regulation No. 5/2020 on Electronic System Organizers (ESOs) in the Private Sector are subject to dynamic debates, not only in Indonesia but in other countries across the world. On one hand, there is a legitimate need from government agencies to access the data of ESOs or digital platforms. On the other hand, basic principles that become the basis of such an access are required to ensure that human rights and personal data protection are well-protected.

"On one hand, there is a legitimate need from government agencies to access the data of ESOs or digital platforms. On the other hand, basic principles that become the basis of such an access are required to ensure that human rights and personal data protection are well-protected."

MOCI Regulation No. 5/2020 essentially discusses some of these principles. For example, it states that there is a need for assessment of the supervision purposes, proportionality, and legality, and that the scope or type of electronic data that are going to be accessed should be described explicitly. Access can only be used for purposes as written in the request. Moreover, the principles of personal data protection and information security are also mentioned explicitly.

Nevertheless, more detailed principal and operational provisions are needed to ensure the protection of human rights and users' personal data. With that as a rationale, this paper suggests several recommendations as follows.

The need for improvements to ensure the due process of law, especially in these aspects:

a. Legality: access to data and electronic systems is related to the basic principles of human rights, personal data protection, and ESOs' trade secret protection. Therefore, regulations on these areas should be made at the Law level. Regulation at the Law level allows for a discussion space by involving the representatives at the parliament. Reflecting from the experiences of South Korea, India, and Brazil, although these countries use different approaches, they have similarities in terms of the existence of a legal basis at the Law level. China's Golden Shield project is the only program that has no clear legal basis, facing objections from the stakeholders.

b. Authorization or stipulation from judiciary/independent bodies: The MOCI Regulation No. 5/2020 differentiates between data that require a court determination letter and those that do not. This is not in line with the spirit of the Indonesian Criminal Procedure Code that requires a court determination letter for a confiscation and search, with the exception of urgent instances. The regulation should adopt this spirit, in which all accesses require a stipulation from the court or other independent bodies, except for certain matters that are described specifically in the Law.

c. Review and appeal: As a case develops, it is possible that an ESO challenges or appeals against an access request. To ensure the protection of both the users' human rights and ESO's basic rights, an avenue is needed to review or lodge an appeal through a neutral body or forum, such as the court. This is similar to the pre-trial review in the Indonesian Criminal Procedure Code, or the review forum on the decision of access rights through an administrative trial.

The MOCI should serve as an advisory body and protector to ensure that access by ministries/government agencies are in accordance with the principles of personal data protection.

Considering that there is a plethora of provisions in sectoral Laws, access by ministries/government agencies can allow for multi-interpretations on government agencies that are authorized to access. It is ideal that the Personal Data Protection Law to be issued before the access right authority by the government can work properly. In the current situation, the MOCI needs to place the MOCI Regulation No. 5/2020 as a policy instrument that ensures that every access request from ministries/government agencies are in accordance with the principles of personal data protection and information security. The MOCI should make the regulation a technical rule that addresses the operation of relationship between the MOCI and law enforcement authorities and other ministries/government agencies (including the civil servant investigators and National Crypto and Cyber Agency), all of which still exercise their practices in the field, rather than making it a creator of new norms.

Access to ESO's system should be chosen as a last resort after other risk mitigation measures have been carried out.

The MOCI Regulation No. 5/2020 does not describe the objectives of access to systems and in what situation it is deemed necessary. Access to electronic systems is not the best practice in information security because it opens a new lapse that poses risks for ESOs' systems. Access to system must comply with international regulations, such as the ISO/SNI SMPI, especially in relation to access control and security operations. Regarding this, government agencies that wish to access the system should comply and be audited using the SMPI Standards before accessing an ESO's system.

REFERENCE

Abraham, S. (2017). Systematic Government Access to Private- Sector Data in India. In F. H. Cate & J. X. Dempsey (Eds.), *Bulk Collection: Systematic Government Access to Private-Sector Data* (pp. 259–274). Oxford University Press. https://oxford.universitypressscholarship.com/view/10.1093/oso/9780190685515.001.0001/oso-9780190685515-chapter-12

Accenture. (2016). *The Ethics of Data Sharing: A guide to best practices and governance*.

Ackerman, S. (2014, January 27). *Tech giants reach White House deal on NSA surveillance of customer data*. https://www.theguardian.com/world/2014/jan/27/tech-giants-white-house-deal-surveillance-customer-data

Columbia University Global Freedom of Expression. (2016, July 14). *Microsoft v. United States. Case Law*. https://globalfreedomofexpression.columbia.edu/cases/microsoft-v-united-states/

Cornell Law School. (n.d.). *National Security Letter.* Retrieved April 30, 2021, from https://www.law.cornell.edu/wex/national_security_letter

Daskal, J., & Woods, A. K. (2015, November 24). *Cross-Border Data Requests: A Proposed Framework - Just Security.* https://www.justsecurity.org/27857/cross-border-data-requests-proposed-framework/

Department of Justice. (n.d.). *Electronic Communications Privacy Act of 1986 (ECPA)*. Retrieved April 30, 2021, from https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1285

Facebook. (n.d.). *Information for Law Enforcement Authorities*. Retrieved April 30, 2021, from https://www.facebook.com/safety/groups/law/guidelines/?_rdr

Global Network Initiative. (2018). *Implementation Guidelines for the Principles on Freedom of Expression and Privacy*. https://globalnetworkinitiative.org/wp-content/uploads/2018/08/Implementation-Guidelines-for-the-GNI-Principles.pdf

Google. (n.d.). *How Google handles government requests for user information*. Retrieved April 30, 2021, from https://policies.google.com/terms/information-requests

Jong, S. J. (2017). Systematic government access to private-sector data in the Republic of Korea. In F. H. Cate & J. X. Dempsey (Eds.), *Bulk Collection: Systematic Government Access to Private- Sector Data* (pp. 287–303). Oxford University Press. https://doi.org/10.1093/idpl/ipt030

Magrani, B. (2017). Systematic Government access to private-sector data in Brazil. In F. H. Cate & J. X. Dempsey (Eds.), *Bulk Collection: Systematic Government Access to Private-Sector Data* (pp. 129–146). Oxford University Press. https://doi.org/10.1093/idpl/ipt033

Nissenbaum, H., Strandburg, K., & Brennan-Marquez, K. (n.d.). *Metadata Project*. Retrieved April 30, 2021, from https://www.law.nyu.edu/centers/ili/metadataproject

OECD. (2019). *Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies*. https://www.oecd-ilibrary.org/sites/15c62f9c-en/index.html?itemId=/content/component/15c62f9c-en

Rubinstein, I. S., Nojeim, G. T., & Lee, R. D. (2014). Systematic government access to personal data: a comparative analysis †. *International Data Privacy Law*, *4*(2). https://academic.oup.com/idpl/article/2/4/195/676962

Schwartz Hannum PC. (2015). *Stored Communications Act Does Not Permit Service Providers to Disregard Subpoenas for E-Mails | Schwartz Hannum PC*. http://www.shpclaw.com/Schwartz-Resources/stored-communications-act-does-not-permit-service-providers-to-disregard-subpoenas-for-e-mails?p=11399

Smith, B. (2016, April 14). *Keeping secrecy the exception, not the rule: An issue for both consumers and businesses*.

https://blogs.microsoft.com/on-the-issues/2016/04/14/keeping-secrecy- exception-not-rule-issue-consumers-businesses/#sm.00001qg545hu8ldwmw7h8092g7f67

Turner, S. A. (2016). *Are Changes in Store for the Stored Communications Act?* http://www.ca6.uscourts.gov/opinions.pdf/10a0377p-06.pdf.

van Eijk, N. (2017). Standards for Independent Oversight. In F. H. Cate & J. X. Dempsey (Eds.), *Bulk Collection: Systematic Government Access to Private-sector Data* (pp. 381–393). Oxford University Press. https://oxford.universitypressscholarship.com/view/10.1093/oso/9780190685515.001.0001/oso-9780190685515-chapter-20

Wang, Z. (2017). Systematic government access to private-sector data in China. In F. H. Cate & J. X. Dempsey (Eds.), *Bulk Collection: Systematic Government Access to Private-Sector Data* (pp. 241–258). Oxford University Press. https://doi.org/10.1093/idpl/ips017

Yeh, B. T., & Doyle, C. (2006). *USA PATRIOT Improvement and Reauthorization Act of 2005: A Legal Analysis*.

ABOUT AUTHOR

Ajisatria Suleiman is a regulatory affairs practitioner specializing in the digital economy and digital finance. He has assisted regional and national internet as well as digital finance industry associations, international development agencies, global tech companies, and local startups.

His research interests cover personal data protection, digital sovereignty, and digital finance.

He is trained as a lawyer with a bachelor's degree from the University of Indonesia, and a master's degree from Erasmus University of Rotterdam and University of Hamburg.

JOIN OUR SUPPORTERS CIRCLES

Through our Supporters Circles, you, alongside hundreds of others, enable us to conduct our policy research and advocacy work to bring greater prosperity to millions in Indonesia.

Those in our Supporters Circles get the opportunity to engage in the work of CIPS on a deeper level. Supporters enjoy:

- Invitation to CIPS' annual Gala Dinner
- Exclusive Supporters-only briefings by CIPS leadership
- Priority booking at CIPS-hosted events
- Personal (Monthly/Quarterly) Supporters-only update emails and videos
- Free hard copy of any CIPS publication upon request

For more info, please contact anthea.haryoko@cips-indonesia.org.

Scan to join

ABOUT THE CENTER FOR INDONESIAN POLICY STUDIES

Center for Indonesian Policy Studies (CIPS) is a strictly non-partisan and non-profit think tank providing policy analysis and practical policy recommendations to decision-makers within Indonesia's legislative and executive branches of government.

CIPS promotes social and economic reforms that are based on the belief that only civil, political, and economic freedom allows Indonesia to prosper. We are financially supported by donors and philanthropists who appreciate the independence of our analysis.

KEY FOCUS AREAS:

Food Security & Agriculture: To enable low-income Indonesian consumers to access more affordable and quality staple food items, CIPS advocates for policies that break down the barriers for the private sector to openly operate in the food and agriculture sector.

Education Policy: The future of Indonesia's human capital need to be prepared with skills and knowledge relevant to the 21st century. CIPS advocates for policies that drive a climate of healthy competition amongst education providers. Such competition will drive providers to constantly strive to innovate and improve education quality for the children and parents they serve. In particular, CIPS focuses on the improvement of operational and financial sustainability of low-cost private schools who serve the poor.

Community Livelihood: CIPS believes that strong communities provide a nurturing environment for individuals and their families. They must have the rights and capacities to own and manage their local resources and to ensure healthy and sound living conditions for the development and prosperity of the community.

www.cips-indonesia.org

facebook.com/cips.indonesia

@cips_id

@cips_id

Center for Indonesian Policy Studies

Center for Indonesian Policy Studies

Jalan Terogong Raya No. 6B
Cilandak, Jakarta Selatan 12430
Indonesia