CFIEC
Center for International Economic Collaboration

Forming Rules for Government Access: Toward Optimizing the International Flow of Personal and Non-Personal Data

Report from Study Group on Government Access and Trade Rules

November 2022

Center for International Economic Collaboration

Summary

If the government improperly uses data held by the private sector (government access), this may create a direct impediment to international data flow and undermine the trust of data subjects and the private sector that support data utilization. Although necessary and beneficial government access should be possible, clarifying the evaluation criteria and creating a shared set of rules is necessary. Inadequate, unclear, and inappropriate rulemaking negatively impacts the development, maintenance, and expansion of data-related businesses.

For example, if the government improperly and forcibly intervenes in private-sector data management policy, it will probably be forced to respond with actions that are incompatible with safety management measures as well as confidentiality obligations based on other legal obligations, contracts, and operational policies. Moreover, even if some level of government access is justified, demands that exceed the limits of the private sector's voluntary data provision may make it difficult to conduct sound business activities and manage data appropriately. Internationally, different criteria are used by countries and regions to determine the scope of government access to data in the private sector. Meeting these varying criteria will increase both management costs and risks.

Japan's concept of DFFT (Data Free Flow with Trust) has a positive impact on international discussions at the G7, G20, OECD, and other organizations, and government access is considered an important element of the concept. To reduce international friction arising from different ideas about the scope and conditions of appropriate government access, and in accordance with elements conducive to future discussions on appropriate rule formation (hereinafter, "safeguards"), parties should begin discussing the shared criteria that will determine necessary and legitimate government access.

This report summarizes the discussions of a study group established within the Center for International Economic Collaboration (CFIEC), but it does not directly propose rules for government access per se. The main focus is on providing an overview of the current understanding regarding the significance and necessity of safeguards, even as discussions clarify them further. Moreover, although the ongoing discussion about government access is mainly concerned with personal data, the distinction between personal and non-personal data is not absolute. Consideration of aspects other than the protection of personal information, such as trade in the digital field, the economy and other aspects of security, intellectual property

protection, and data-driven innovation, is equally important. Regarding supporting international data flow, a comprehensive perspective that includes both personal and non-personal data is necessary. Such a perspective anticipates that diverse viewpoints coexist in an increasingly complex international situation and carefully provides an overview to avoid arbitrarily excluding differences in specific ideologies and polities.

The reality is that government access takes many different forms, including discussions about the perceptions of legitimacy caused by differences in legislation designed to protect personal information as well as concerns that stem from differences in how national sovereignty relates to data maintenance and management. Regarding what data held by the private sector should be accessible to the government, our discussion suggests that care must be taken when broadening the scope of existing discussions to go beyond just personal information. As much as possible, bias in identifying issues and discussions about safeguards must be avoided. Assuming the following classification foci will assist in that process.

Classification of Government Access

1. Classification by data type: data type (personal or non-personal, including ambiguous types), nature of the data (e.g., 3Vs: volume, variety, velocity), data value (intellectual property, etc.)
2. Classification by degree of enforcement: is it compulsory regardless of the penalties involved and is it voluntarily or spontaneously provided by the private sector
3. Data lifecycle classification: do issues that arise refer to actions taken at the time of data acquisition, or is use after acquisition, provision to non-governmental authorities, alteration, or deletion anticipated
4. Classification by data flow: will data flow directly to the government sector or to organizations designated by the government sector, including certain private sector entities
5. Classification by the cross-border nature of issues: are issues limited to the relevant country or region, or are they due to demands that cross two or more countries and regions

6. Classification by purpose of government access: what purposes are assumed for government access, such as criminal investigation, security, domestic industry promotion, and the protection of citizens' personal information

These six classification foci recognize the breadth of anticipated issues with government access, but foci 1, 2, and 5 in particular characterize the nature of government access.

Based on the foci listed above, we analyzed a wide range of cases, expanded the scope while still referring to existing discussions on government access, and presented 14 items as elements required for appropriate rule formation in the future (safeguards). The first seven items are based on existing discussions and we add our own discussions regarding their significance, while the remaining items are discussed based on our review. To present many points that can contribute to future rule discussions, we risked overlapping meanings and content across the items. These safeguards should not unconditionally be included in discussions, but will be referenced as necessary for the purpose of confirming candidates or comprehensiveness when appropriate.

Examples of expanded safeguards that should be considered in government access involving non-personal data

1. Legal basis: There should be a valid legal basis in the country where data is accessed (e.g., the country whose government is requesting data; or where data are held by the private sector.)
2. Meet legitimate aims and be carried out in a necessary and proportionate manner: The purpose of government access should be justified and the measures taken should be both necessary and proportionate
3. Transparency: The content and process of government access should be explicit, especially for the private sector providing the data
4. Approvals and constraints: Government access should be approved and constrained in scope
5. Limitations: There should be clear restrictions on the minimum handling and maintenance of data

6. Independent oversight: Supervision and approval by an independent body should be a pre-condition
7. Effective redress: There should be clear mechanisms for challenging and seeking redress against unlawful or inappropriate government access
8. Impartiality and non-discrimination: Partial and discriminatory treatment should be eliminated in the selection of private actors to be accessed by government
9. Uniformity: The application of the legal system for government access should not be arbitrary; it should be carried out using uniform standards and methods
10. Fair and equitable treatment: Treatment must not be arbitrary, unfair, unjust, or idiosyncratic, and should not be based on prejudice or discrimination due to factors such as race, ethnicity, culture, religion, place of residence, or gender
11. Economic rationality: It should not impose excessive costs or burdens on the private actor subject to government access or on society
12. Compensation: Substantial compensation should be provided upon request to companies subject to government access as well as individuals affected financially
13. Limitation of liability: The various liabilities that may arise as a result of a private actor's compliance with government access should be limited or waived for the relevant private actor
14. Conflicts of law: If there is another law or regulation that conflicts with the legal basis for government access, either domestically or internationally, the government should be responsible for handling potential contradictions and conflicts, both before and afterward

In this report, these 14 safeguards are analyzed individually while considering the relevant evaluation criteria. The evaluation criteria for each discipline element are designed to function as indicators to help the government consider potential protective legal benefits and loss of benefits by any party (individual, private sector, or society) as a condition for accepting the relevant government access. We also provide an analysis of the significance of incorporating the relevant safeguards, their relationship to other safeguards, and their relationship to other international rules.

We expect this report to be used in international discussions and that the prospective readers will be policymakers and corporate practitioners. Care should be taken with the scope of the word "access," as it is necessary to discuss not only the forms of data acquisition that can be used exclusively by governments or government agencies, but also arbitrary restrictions on access by others, alterations of the data itself, falsification requests, deletions, concealment, and so forth, in the broad sense of "access."

In parallel with the international rulemaking that is likely to continue, it is also important to consider existing international rules such as the WTO Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) as well as the handling of illicit government access based on the national laws of the countries and regions where the access is taking place. Furthermore, as a way to collect evidence for rulemaking discussions, quantitative investigation and analysis of the negative economic impact of government access is necessary.

If government access goes unchecked, data held by the private sector and data subjects will effectively be controlled by the government and government agencies. Determining who should be considered the subject of data governance is important for the utilization and free flow of data. Here, too, it is necessary to respect the philosophy of multi-stakeholders; examine the roles and powers of the government, the private sector, and data subjects; and achieve universal understanding through a clarification of the division of duties. Referring to the 14 safeguards identified in this report, it must be ensured that government access does not adversely affect the digital economy, the sound development of innovation, or the resolution of social issues.

November 2022

Center for the International Economic Collaboration

Study Group on Government Access and Trade Rules

Committee members (affiliations when the study group was formed)

Naoto Ikegai	Hitotsubashi University
Kaori Ishii	Chuo University
Yoichiro Itakura	Attorney at law (Hikari Sogoh Law Offices)
Shigeo Takakura	Meiji University
Jun Nakatani	JEITA Trade Committee
Taku Nemoto	OECD Trade and Agriculture Directorate
Kenta Hirami	Waseda University
Yu Yamada	Japan Business Federation
Mariko Watanabe	Gakushuin University

Moderator

Makoto Yokozawa	Center for International Economic Collaboration

Observer

Ministry of Economy, Trade and Industry

1. The Study Group's Problem Awareness, Objectives, and Consideration Policy

1.1. The Study Group's Problem Awareness

As shown by concepts such as Society 5.0, which the Japanese government has advocated for, businesses that utilize data are indispensable for future economic development and solving social issues. If data flow, which is at the core of this development, is hindered, it will be difficult to operate businesses based on data. As many industries depend on data and digital transformation, an impediment here could have a negative impact on a wide range of industries.

With a view toward addressing the potential adverse effects described above, Japan's basic policy of promoting data flow, "Data Free Flow with Trust" (DFFT), advocates for synergistic effects between "trust" and "free flow" by further promoting the free flow of data. This is done by addressing issues related to privacy, intellectual property rights, and security, as well as by strengthening consumer and business trust.[1]

Inappropriate access to privately held data by public authorities (government access) carries the risk of infringing on privacy and intellectual property rights, while violating "trust" in data distribution might obstruct the free flow of data. This could create a vicious cycle.

There are currently no internationally agreed-upon rules about government access covering both personal and non-personal data, but the Committee on Digital Economic Policy (CDEP) of the Organization for Economic Co-operation and Development (OECD) is currently considering safeguards with respect to personal data.[2]

However, personal data is inherently fluid, meaning that a complete separation of personal and non-personal data is not possible. The definition of personal data itself may differ based on the data protection system in various countries. It is not easy for companies to distinguish between personal and non-personal data. For example, it has been pointed out that most information must be treated as personal information under the EU's General Data Protection Regulation (GDPR), while in other countries personal data is treated as non-personal data through

[1] Ministry of Internal Affairs and Communications, "Comprehensive Data Strategy" (June 2021), p.50. https://www.soumu.go.jp/main_content/000756398.pdf (retrieved August 22, 2022)
[2] OECD "Government access to personal data held by the private sector: Statement by the OECD Committee on Digital Economy Policy," https://www.oecd.org/digital/trusted-government-access-personal-data-private-sector.htm (retrieved August 22, 2022)

anonymization. Thus, government access to both personal and non-personal data is an important issue.

There has also been an increase in legal systems used by states to manage non-personal data, such as the Indian Non-Personal Data Governance Framework, the European Data Governance Act and Data Act, and China's data-related laws (Cyber Security Law, Data Security Law), meaning that government access to non-personal data is proceeding without international agreement. This increases the necessity of discussing regulations for government access to non-personal data.

Considering the current state of international rule formation, it would be beneficial to establish government access rules that cover both personal and non-personal data as trade rules. As mentioned above, government access can have a major impact on cross-border business, with World Trade Organization (WTO) agreements governing the provision of goods and services across borders, and e-commerce negotiations progressing at the WTO as one of the ways to realize DFFT. Recently, rules related to digital trade have been developed in the e-commerce chapters of Free Trade Agreements or Economic Partnership Agreements (FTAs/EPAs), including rules for handling data (data free flow, prohibition of domestic installation of servers (data localization), etc.), which are framed as a way to promote DFFT.

As such, it is necessary to focus on rules for state conduct with respect to data that could affect cross-border business, and to incorporate government access into trade rules as part of digital trade rules.

1.2. The Study Group's Objectives and Consideration Policy

This report is based on a summary of the discussions held by a study group established within the Centre for International Economic collaboration. As a basic study for establishing trade rules in the future, the study group aimed to present ideas on safeguards for government access to both personal and non-personal data to ensure data free flow. It was also considered important for the protection of data subjects that the safeguards be meaningful to the private sector.

For this reason, the study group took four steps: (1) understand the reality of government access, (2) analyze the discrepancies between the rules required for personal and non-personal

data, (3) discuss the criteria for evaluating safeguards, and (4) identify elements that should be added or removed from non-personal data safeguards. Using this as background, we present our ideas on safeguards for government access.

Assuming a standpoint of global rulemaking, our consideration policy was aimed at formulating rules so that specific states (for example, countries with certain political systems) would not be uniformly excluded. Moreover, in terms of establishing trade rules, we decided to incorporate safeguards designed specifically to eliminate business obstacles.

2. Collection and Analysis of Case Studies for Considering Government Access Rules

2.1. Selection Criteria for Cases to Be Analyzed

When considering safeguards, it is important to protect the rights and interests of individuals and the private sector as well as to prevent adverse effects on cross-border data flow. As such, it is appropriate to keep three specific items in mind that are thought to have a particular impact: the types of data, enforcement, and the cross-boundary nature of issues.

- **Types of data**
  It is important to consider non-personal data in terms of safeguards for both non-personal data and other types of data. This is also a factor when considering the three Vs (volume, variety, velocity),[3] which are generally referred to as data characteristics. The impact of violating the interests of individuals and the private sector whose data are accessed will differ depending on the data's volume, variety, and velocity.
  From this point of view, we were able to select government access cases that comprised information with high intellectual property value, such as drug test data, real-time automobile travel information, and health and sales information. At the same time, we selected government access cases based on fixed-point observational data.

[3] Marbella International University Centre "The Vs of Big Data," May 2020, https://miuc.org/vs-big-data/ (retrieved August 22, 2022)

- **Enforcement**

  In the case of voluntary provision, violations of interests are unlikely as the individual or the private sector submitting the data gives their consent. Violation of rights and interests becomes an issue because the distinction between enforcement and voluntary is not uniform. However, enforcement can take many forms. For example, in addition to legal obligations, data can be provided in exchange for permits and licenses, making data provision voluntary but including background enforcement elements.

  For the case studies described below, along with those that are legally obligated, we have selected cases that concern de facto enforcement, such as business disadvantages being imposed if the subject does not comply, as well as those where concerns are extremely weak or non-existent (the government requests voluntary submission).

- **Cross-boundary nature of issues**

  Although issues often arise in such a way that they are limited to a single country or region, it is important to discuss the impact on cross-border data free flow. When it comes to espionage by foreigners in foreign countries, which has been reported to occur extrajudicially, it is often difficult to get a reliable overview of the situation.

  Cases selected under these criteria include ones where there is access to data that has been transferred from abroad as well as cases where there is concern that such access may take place. Furthermore, the country in which the government access occurs provides a geopolitical dimension. In terms of promoting business, we can analyze cases conducted by emerging countries that have had adverse effects on business and cases in developed countries (the United States and EU countries) that are regularly brought up in international discussions.

2.2. Cases of Government Access

Case studies were collected and analyzed to extract elements that would contribute to future discussions on appropriate rule formation (safeguards). Descriptions are based on those available at the time the information was provided. It is possible that, in some cases, the legal system has been revised, implementation has changed, or that issues may have been resolved or been alleviated since that time. Moreover, some content is based on the observations of the referencing reporter, meaning that alternative observations may be possible in some situations, but we have tried to include a description from as flexible a perspective as we can.

Case 1 【China】 Requests for disclosure of confidential technical information in exchange for administrative approval

Case 2 【China】 Prohibition of cross-border transfer of data collected by automobiles

Case 3 【China】 Acquisition of voice data by the government for national security purposes

Case 4 【India】 Mandatory sharing of non-personal data (framework for creating and using high-value datasets)

Case 5 【US-EU】 Access to data transferred from the EU for the purpose of US government surveillance (Schrems I/II)

Case 6 【US-EU】 Requests for disclosure of data from abroad relevant to criminal investigations (Microsoft case, CLOUD Act)

Case 7 【China】 Concerns about unlimited data acquisition by government under the National Intelligence Law

Case 8 【Singapore】 Use of COVID-19 control app data for criminal investigations

Case 1 【China】 Requests for disclosure of confidential technical information in exchange for administrative approval

The Chinese government was directly or indirectly forcing foreign companies (especially in high-tech industries) to transfer technology in exchange for access to the domestic market.

In March 2018, the Office of the US Trade Representative (USTR) released an investigative report[4] on the unfair, irrational, and market-distorting laws and practices of the Chinese government that aimed to upgrade its industry by acquiring technologies and intellectual property from foreign companies. Based on this, the US government invoked tariffs as policy measures.

The report points to requests for the disclosure of classified technical information in exchange for necessary administrative approvals as one of the technology transfer mechanisms used by the Chinese government. Foreign enterprises in various industries such as ICT, pharmaceutical, chemical, agri-food (especially genetically modified crops), machinery, financial services, and so forth can obtain permission for factory construction and product sales, requiring them to provide detailed information to government agencies. In some cases, such corporate information has been provided to local industries and used for similar industrial activities. There have also been concerns that disclosed information might be given not only to the government but also to third parties after being reviewed by expert panels (composed of representatives of government, industry, academia, etc.) that may involve competing relevant stakeholders. Such expert panels might make review requests in a variety of industries at any stage of a company's operation in China. The revised USTR report states that high-tech industries, particularly aerospace and chemical companies, have faced strong pressure to transfer technology.[5]

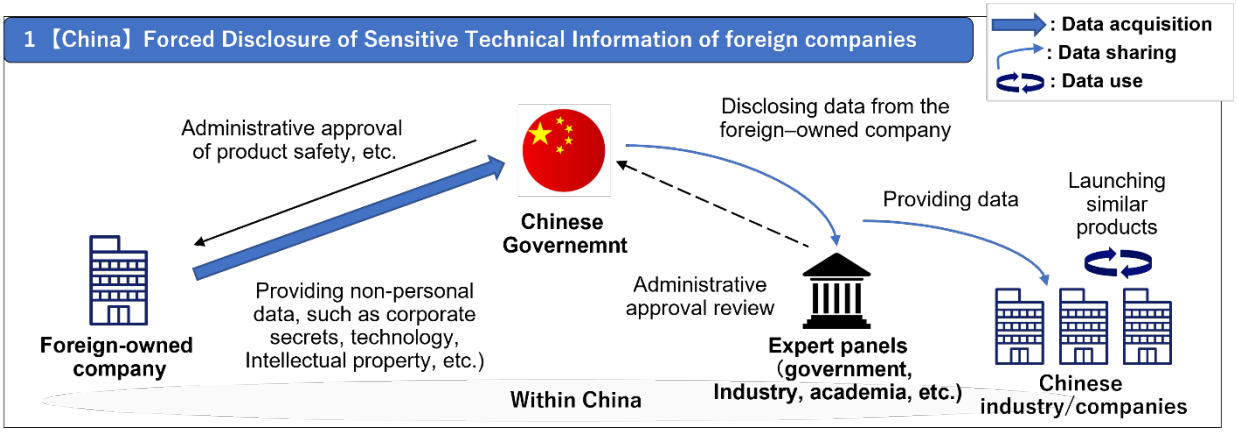
The US government has filed a complaint with the WTO Dispute Settlement Body about discriminatory treatment by the Chinese government.[6] In response to these developments in other countries, China has revised its law, and forced technology transfer has been prohibited according to the Foreign Investment Law of 2019. The Data Security Law of 2021 sets the

[4] The Office of the United States Trade Representative (USTR), "Findings of the Investigation into China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation under Section 301 of the Trade Act of 1974," March 2018.

[5] The Office of the United States Trade Representative (USTR), "Update Concerning China's Acts, Policies and Practices Related to Technology Transfer, Intellectual Property, and Innovation," November 2018, p.23.

[6] Ibid., p.5.

standard for data processing activities in China, and stipulates data security assurances, personal and organizational protection obligations, penalties, and so forth.[7]



Source：The Office of the United States Trade Representative (USTR), "Findings of the Investigation into China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation under Section 301 of the Trade Act of 1974", 2018. Figure based on source material.

Case 2 【China】General prohibition of cross-border transfer of data collected by automobiles

The Chinese government banned cross-border transfer of data collected about automobiles.

In China, the Cybersecurity Law was enacted in 2017, while the Chinese Data Security Law and the Chinese Personal Information Protection Law were enacted in 2021, thus establishing China's three data protection laws.[8]

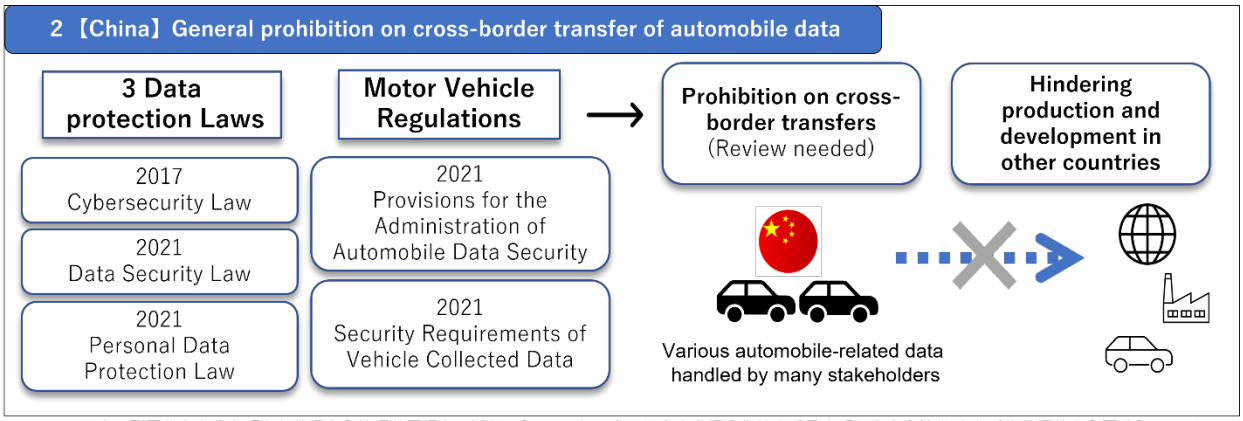
In response to these developments, the following bylaws were enacted one after another; "Certain Provisions for the Administration of Automobile Data Security (Exposure Draft)"[9] were announced for the automobile industry in August 2021, followed by "Information Security

[7] Motoo Yuno, "Establishment of the Data Security Law in China" (*Foreign Legislation*, No. 289–1, October 2021) https:dl.ndl.go.jp/view/download/digidepo_11767245_po_02890113.pdf?contentNo=1 (retrieved August 22, 2022)

[8] The Chinese names of the three data protection laws are as follows, in the order in which they are described.
「中华人民共和国网络安全法」「中华人民共和国数据安全法」「中华人民共和国个人信息保护法」

[9] 国家互联网信息办公室『汽车数据安全管理若干规定(试行)』 (announced August 16, 2021) http:www.cac.gov.cn/2021-08/20/c_1631049984897667.htm
(Reference website with Japanese translation: http:maruyama-mitsuhiko.cocolog-nifty.com/security/2021/08/post-fefed0.html?fbclid=IwAR1iu43oAGFGt8-MSFQ6A5JdgmbC2KS_vJLiCIBtaA1b1qiB05dTN3i51LE) (retrieved August 22, 2022)

Technology —Security Requirements of Vehicle Collected Data"[10] in October 2021. In both cases, cross-border transfer of automobile data is prohibited in principle, and in cases where it is necessary to transfer data across a border, it must pass the cross-border data security assessment conducted by the National Cyberspace Administration.[11] The category of "automobile data and automobile data processors" is broad,[12] and it can be said that the scope of data acquisition is too broad in proportion to the stated purpose. Moreover, it has hindered production and development by Japanese automakers. On the other hand, "Certain Provisions Concerning the Security Management of Automobile Data (Trial)" (Article 11) states that "if there are different provisions in an international treaty or agreement to which China is a party, the international treaty or agreement shall apply, excepting those provisions that China has declared that it shall defer." This suggests that treatment might differ in cases where there is an international agreement.



Source：国家互联网信息办公室『汽车数据安全管理若干规定（试行）』(2021年) 全国信息安全标准化技术委员会『信息安全技术 汽车采集数据的安全要求』(2021年)
Figure based on source material.

[10] 全国信息安全标准化技术委员会『信息安全技术 汽车采集数据的安全要求』 (October 2021)
https:www.tc260.org.cn/file/2021-10-19/e5a87bcd-770f-4035-83dd-610e15a34096.pdf
(Reference website with Japanese translation: http:maruyama-mitsuhiko.cocolog-nifty.com/security/2021/10/post-69a493.html) (retrieved August 22, 2022)
[11] Ibid. (9) (Article 11) and Ibid. (10) (Article 7)
[12] Ibid. "(9) (Article 3) In this provision, automobile data includes data pertaining to personal data and important data in the process of design, production, sale, use, operation and maintenance of automobiles. […] Automobile data processors refers to organizations that carry out automobile data processing, such as automakers, parts and software suppliers, dealers, repair shops, and travel service companies. […] Important data means data that, at the time of alteration, destruction, leakage, unauthorized access, or unauthorized use, may threaten national security, public interests, or the legitimate rights and interests of an individual or organization."

Case 3 【China】 Acquisition of voice data by the government for national security purposes

China is building a nationwide voice recognition database for the purpose of national security.

In China, digital strategies are being promoted from the top down, and the government is simultaneously creating public-private sector integrated innovation by fully supporting private companies in priority industries in terms of funding and policy.[13] In July 2017, the Ministry of Science and Technology of China formulated the "Next Generation Artificial Intelligence (AI) Development Plan." To realize innovation using AI, four priority areas (1. autonomous driving, 2. smart cities, 3. healthcare, and 4. voice recognition) were defined, with leading companies selected for each field.

The Chinese government is collecting personal voice authentication data (biometric data) to build a national voice authentication database for the purposes of counterterrorism and public security by utilizing AI technology that has been developed with significant government support.[14] A leading company in the field of speech recognition is cooperating with the Ministry of Public Security to build a national voice pattern database and develop a pilot version of a surveillance system that can automatically identify the voice of a person of interest from a phone call. The involved company is also a designated supplier of voice pattern collection systems purchased by police stations in the provinces of Xinjiang and Anhui. It offers commercial text-to-speech and recognition apps for mobile phones in China, but the large voice datasets from the apps could also be used for monitoring. It is unclear to what extent the company shares personal information collected for commercial purposes with the Ministry of Public Security, but the company says it may disclose personal information at the request of relevant government departments.

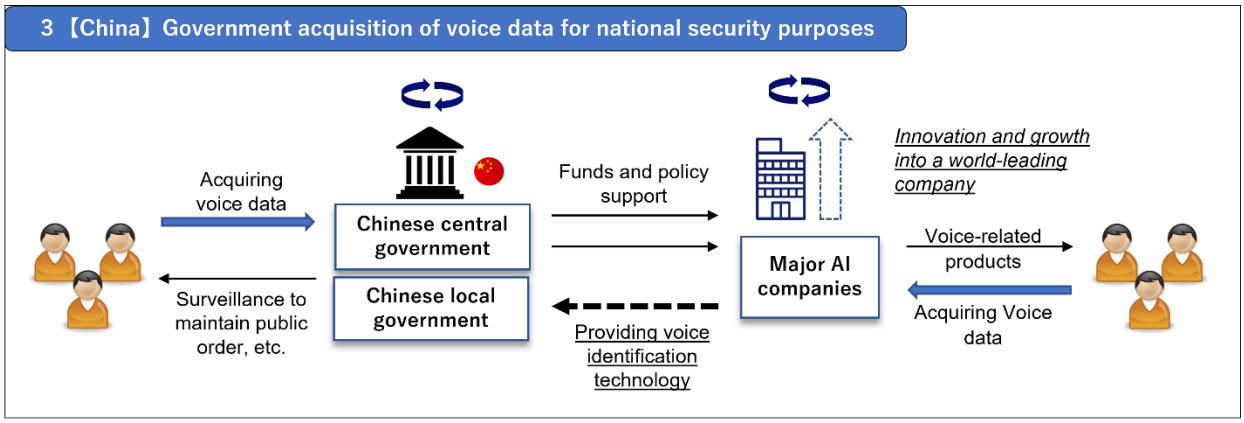
In a 2017 report, a China representative at Human Rights Watch said, "The Chinese government collects the speech patterns of tens of thousands of people, but there is little transparency about the program or the laws that govern the people targeted and how that

---

[13] Zhihui Lee, "Formation and Development of China's Digital Powerhouse Strategy" (*Overseas Investment and Loans*, September 2021) pp.20-26.; Mitsubishi Research Institute, "Trends toward the Social Implementation of Artificial Intelligence in China," https:www.soumu.go.jp/main_content/000483136.pdf (retrieved August 22, 2022)
In the field of speech recognition, companies have been improving speech recognition technology by utilizing enormous volumes of high-quality data accumulated by the government as training data.

[14] Human Rights Watch, *China: Collecting Voice Authentication, Data Privacy Threats: The Police Major AI Companies Working together in a Legal Gray Zone* (October 2017) https:www.hrw.org/ja/news/2017/10/23/310343 (retrieved August 22, 2022)

information is used." They have pointed out that in China, with its continuous unchecked surveillance and retaliation against government critics, it is easy for the authorities to collect and potentially misuse data. However, the Data Security Law was enacted in 2021, after which the handling of data related to government access has improved.



Source：Human Rights Watch, 2017, https://www.hrw.org/ja/news/2017/10/23/310343, retrieved August 22, 2022. Figure based on source material.

Case 4 【India】 Mandatory sharing of non-personal data (framework for creating and using high-value datasets)

The Indian government is submitting a report on making the sharing of non-personal data mandatory.

In December 2020, a report on a non-personal data governance framework was submitted by an Indian expert committee.[15] It frames non-personal data as a public good and envisions data sharing as a way to ensure that Indian society gains the greatest value (especially economic benefits) from the data. That report proposes a new framework that requires data-holding entities to share non-personal data.

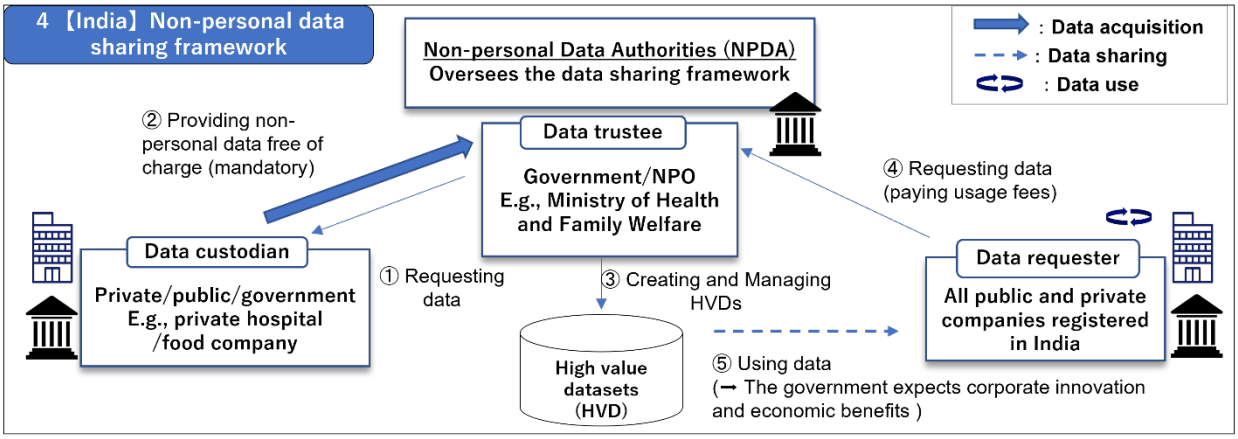
Specifically, it establishes a Non-Personal Data Authority (NPDA) to oversee rules on non-personal data. Within its regulations, data trustees collect data from data custodians and create and manage high-value datasets (HVDs). Any organization registered in India can request HVD data from data trustees. Data trustees may collect fees to cover the costs of data processing and

[15] Ministry of Electronics and Information Technology-Government of India, "Report by the Committee of Experts on Non-Personal Data Governance Framework," 2020.

so forth. The Indian government hopes that the sharing and use of non-personal data will promote innovation in start-ups and others with limited access to data.

However, the mandatory sharing of data has been criticized by researchers and private companies, as well as other concerned parties.[16] First, critics say that it is costly for companies to collect data, but they are required to share datasets free of charge and with no incentives. Compensation for preparing data for use by third parties and for the value of the data should be considered. Companies should also be shielded from liability that might arise from third-party data use. Second, there is a question of whether anonymized data constitutes non-personal data.[17] Data custodians provide data to data trustees after anonymization, but since data regarding individuals is being collected from more data sources, identifying individuals is becoming easier, even with highly anonymized data. Third, existing research has not provided evidence that sharing large datasets promotes innovation.

For these reasons, the establishment of the NPDA in India is a new idea worth considering; however, it is too early for it to be put it into practice, and some have argued that legislation and investment in personal data protection are necessary first.[18]



Source：MEITY-Government of India, "Report by the Committee of Experts on Non-Personal Data Governance Framework", 2020. Figure based on source material.

[16] Jain, R., Pingali, V., "India's Non-Personal Data Framework: A Critique," *CSI Transactions on ICT* 9, 2021, pp.171–183.
[17] The scope of the proposed statute in the NPD report is as follows: all data not covered by "personal data" in the Personal Data Protection Bill, 2019 (PDP Bill 2019).
[18] Kapoor, A., Nanda, A., "Non-Personal Data Sharing: Potential, Pathways and Problems," *CSI Transactions on ICT* 9, 2021, pp. 165–169.

Case 5 【US-EU】 Access to data transferred from the EU for the purpose of US government surveillance (Schrems I/II)

There are concerns that personal data transferred from the EU to the United States is subject to surveillance by US government agencies.

In the EU, the "EU Data Protection Directive"[19] was adopted in 1995, so that transfer of personal data outside the EU was only allowed when the European Commission has issued an adequacy decision for the destination country of the data transfer. Although there was no "adequacy decision" with the United States in this specific case, the US and EU agreed to a "Safe Harbor Agreement," which is a framework for obtaining equal protection. Based on this agreement, only companies authorized by the US Department of Commerce may receive personal information.[20]

However, after the 2013 "Snowden Incident" revealed that the US National Security Agency (NSA) was monitoring and collecting data held by IT companies in the United States, Austrian resident Schrems filed a complaint alleging insufficient protection of his Facebook personal data transferred to the United States (Schrems I[21]). In October 2015, the EU Court of Justice ruled that the Safe Harbor Agreement was invalid[22] because the data transferred from the EU could be accessed by US government agencies beyond what is strictly necessary and proportional for national security, the public interest, and law enforcement. Moreover, since the collection and additional processing of personal data was part of US surveillance programs, the Court deemed that people had no opportunities to access, revise, or delete their own data, or to receive administrative or judicial assistance.

As US companies were no longer able to transfer data under the Safe Harbor Agreement, Standard Contractual Clauses (SCC) and Binding Corporate Rules came to serve as the basis for data transfers, but in July 2016, the European Commission adopted the Privacy Shield[23] as a new

---

[19] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995.

[20] EU MAG, "Launch of a New Framework for the Transfer of Personal Information between the EU and the US" (Vol. 54, October 2016) https:eumag.jp/behind/d1016/ (retrieved August 22, 2022)

[21] CJEU, Maximillian Schrems v Data Protection Commissioner, Case C-362/14, 2015.

For a commentary, see Hiroshi Miyashita, "EU-US Privacy Shield" (*Keio Law Journal*, No. 36, December 2016), pp. 145-179.

[22] ICR – InfoCom Research, "On the European Court of Justice's Judgment on the Invalidity of the Safe Harbor Agreement" (*InfoCom Law Report*, 2015) https:www.icr.co.jp/newsletter/law20151008-fujii.html (retrieved August 22, 2022)

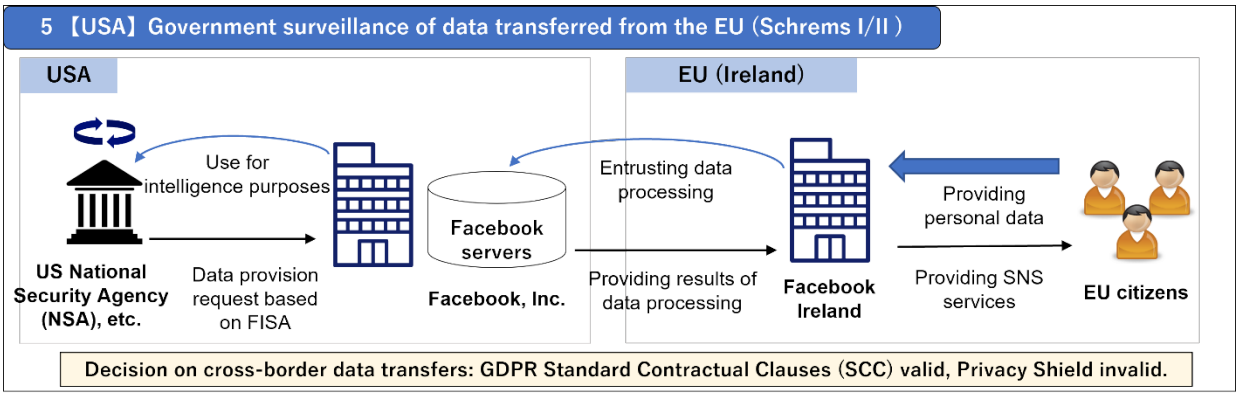
[23] Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the EU-US Privacy Shield (notified under document C(2016) 4176)

transfer framework. The Privacy Shield mandates stronger measures to protect the data of EU citizens, stipulating restrictions on and protection from access by US public authorities.

However, Schrems filed another complaint, citing concerns that even if data is transferred in accordance with the Privacy Shield or SCC, they will not be adequately protected in the United States. Consequently, in July 2020, the European Court of Justice ruled the Privacy Shield framework to be invalid (Schrem II[24]). The reasons for this decision were 1) that it recognizes, as with the Safe Harbor Agreement, that the needs of US national security, the public interest, and law enforcement take precedence over the fundamental rights of data subjects guaranteed under the EU Charter of Fundamental Rights,[25] 2) that Article 702 of the Foreign Intelligence Surveillance Act (FISA), which is the basis for US intelligence activities, and Executive Order (E.O. 12333), are not limited to the minimum extent necessary in view of the principle of proportionality under EU law,[26] and 3) that the system for submitting complaints in the event of infringement is inadequate, not ensuring legal remedies for data subjects.[27] Meanwhile, the European Commission's decision[28] on SCC within the framework of the EU's General Data Protection Regulation (GDPR)[29] was found to be valid. An SCC is the conclusion of a contract with a template clause recognized by the European Commission that faced extremely high hurdles prior to its introduction, but following the invalidation of the Privacy Shield, the European Commission revised the SCC in June 2021.[30] The new SCC addresses a wide range of data transfer scenarios and complex data processing. Moreover, regarding the protection of personal data, they included an article on security assurance to achieve the same level of protection as in the EU. The SCC is also designed to counter risks of personal data violations due to government access, such as requiring the data importer to notify the data exporter when a data access request is received from the government of the country where the data is transferred.

[24] CJEU, Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems, Case C-311/18, 2020)
[25] Ibid., pp.164, 165.
[26] Ibid., p.184.
[27] Ibid., pp.191, 192; For a commentary, see Corporate Legal Navigation "Overview and Impact of the Invalidation of Privacy Shield (Adequacy Decision to the United States): Ruling in Schrems II by the EU Court of Justice (2020) https: www.corporate-legal.jp/news/3604 (retrieved August 22, 2022)
[28] Commission Decision of 5 February 2010 on Standard Contractual Clauses for the Transfer of Personal Data to Processors Established in Third Countries under Directive 95/46/EC of the European Parliament and of the Council (notified under document C(2010) 593)
[29] Japan External Trade Organization (JETRO), "About the EU General Data Protection Regulation (GDPR)," https:www.jetro.go.jp/world/europe/eu/gdpr/ (retrieved August 22, 2022)
[30] European Commission, "European Commission adopts new tools for safe exchanges of personal data," 2021.

According to a survey in late 2020, SCC is the most used international data transfer mechanism, of particular importance for all kinds of businesses in Europe.[31]



Source：Commissioner v. Facebook Ireland and Maximillian Schrems, Case C-311/18, 2020. Figure based on source material.

Case 6 【US-EU】 Requests for disclosure of data from abroad relevant to criminal investigations (Microsoft case, CLOUD Act)

The US government requested the disclosure of data stored outside the country.

In the United States, before the enactment of the Clarifying Lawful Overseas Use of Data Act (CLOUD Act) in 2018, the Stored Communications Act ("SCA" 18 U.S.C. § 2703) [32] and other laws about the procedures for providers of telecommunications services and such to disclose data did not explicitly include stipulations about US government agencies and data stored outside the United States.

In 2013, US law enforcement agencies asked Microsoft to provide certain e-mail information, but Microsoft argued that this was an unlawful extraterritorial application of the SCA as it required disclosure of materials stored abroad, since the storage servers were located in Ireland, and filed a petition for the warrant to be ruled invalid. The US District Court dismissed the petition, but when Microsoft appealed, the US Court of Appeals for the Second Circuit

[31] DIGITALEUROPE, "Schrems II Impact Survey Report," 2020.
[32] 18 US Code Chapter 121 § 2703 - Required Disclosure of Customer Communications or Records.)

recognized the company's argument that the SCA applied to data stored within the United States (Microsoft case).[33]

It was at this point that the US Congress enacted the CLOUD Act,[34] which clearly stated that warrants under the SCA had extraterritorial validity, which meant that the Microsoft case was no longer relevant. The CLOUD Act clarifies that the US government can force providers under US jurisdiction to store, back up, and disclose data they store both domestically and abroad.[35]

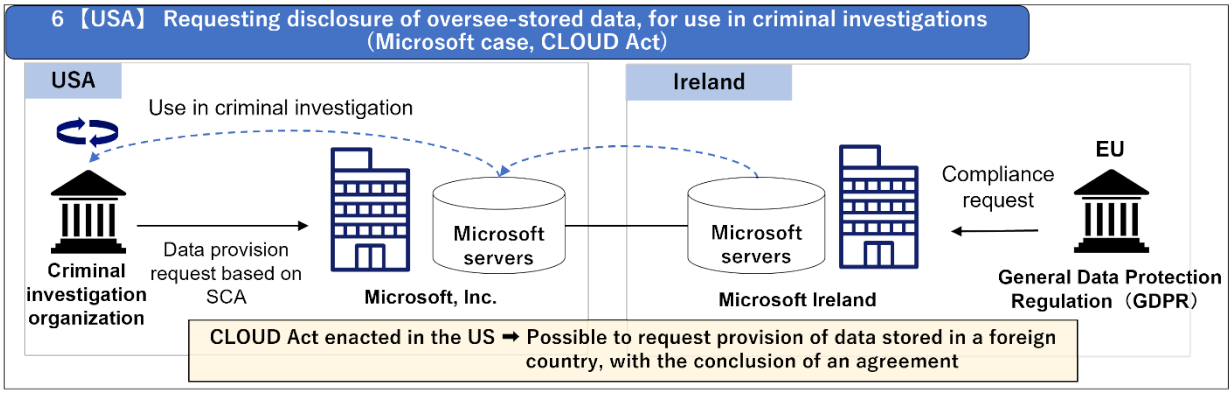
Communications service providers (CSPs) operating globally may be subject to the laws and regulations of multiple countries, which can cause conflicts between one government's data disclosure request and another country's legal obligation to restrict data disclosure.[36] In some cases, such judicial conflicts can be resolved through a so-called mutual legal assistance treaty (MLAT), but since the acquisition of data goes through the courts and governments of other countries, these procedures are complicated and take a long time. The CLOUD Act assumes that the United States will conclude executive agreements with other countries that meet certain standards such as respect for the rule of law and allows the governments of both countries to issue orders to submit electronic data directly to the CSP without having to go through the other government. This eliminates the restrictions under US law and does away with judicial conflicts.

However, an agreement under the CLOUD Act does not impose an obligation on CSPs in the United States and other countries to comply with the orders of other countries' governments, and it holds no jurisdiction over CSPs in other countries.[37] Moreover, data disclosure is limited to purposes related to the prevention and investigation of terrorism and other serious crimes, which means that existing high standards under US law must be met before disclosure of electronic data can be requested by law enforcement agencies. Moreover, a CSP that has received a request to disclose data may file a petition in a US court within 14 days if it reasonably believes that complying with the disclosure would entail a significant risk of violating laws in the other country, allowing it to seek a revision or revocation of the disclosure order.[38]

---

[33] United States v. Microsoft Corp., 829 F.3d 197 (2nd Cir. 2018)
[34] Enacted as part (Division V) of the Consolidated Appropriations Act 2018) on March 23, 2018.
[35] CLOUD Act Sec.3(a)(1), 18 USC. Sec. 2713.
[36] US Department of Justice "Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act," April 2019, pp.2-6.
[37] Ibid., p.5. Moreover, the agreement does not require either government to force companies to comply with orders issued by the other government.
[38] CLOUD Act Sec.3(b), 18 USC. Sec. 2703(h)

If the US government requires a Japanese company to disclose data under the CLOUD Act, this may not be consistent with the Constitution of Japan and other domestic laws (Telecommunications Business Act, Personal Information Protection Act, etc.). Moreover, if Japan concludes an administrative agreement with the United States in the future, while that would facilitate the acquisition of cross-border data for investigation purposes, attention needs to be paid to the impact it may have on other international agreements concluded by Japan. Various legal issues need to be considered to realize the concept of Data Free Flow with Trust (DFFT) and to enable appropriate cooperation with investigations while also protecting data subjects.[39]



Source：United States v. Microsoft Corp., 829 F.3d 197 (2nd Cir. 2018)
U.S. Department of Justice "Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act", 2019.
Figure based on source material.

Case 7 【China】 Concerns about unlimited data acquisition by government under the National Intelligence Law

In June 2017, China's National Intelligence Law came into effect.[40] There have been concerns that under this law, national intelligence agencies would have virtually unlimited government access to related agencies, organizations, and individuals when conducting intelligence activities at home and abroad.

[39] Nishimura Institute of Advanced Legal Studies, *Report of the CLOUD Act Study Group: Consideration of and Recommendations on Legal Issues Surrounding Investigations Involving Data Held by Companies* (December 2019)
[40] Shikako Okamura, "China: Enactment of the National Intelligence Law" (Foreign Legislation, No.272-2, Aug. 2017) https:dl.ndl.go.jp/view/download/digidepo_10404463_po_02720209.pdf?contentNo=1 (retrieved August 22, 2022)

Article 7 of the National Intelligence Law stipulates that all organizations and individuals shall cooperate with the intelligence activities of the state in accordance with the law and shall be obliged to protect the confidentiality of the state's intelligence activities, while the state shall protect the organizations and individuals who have cooperated with the intelligence activities.[41]

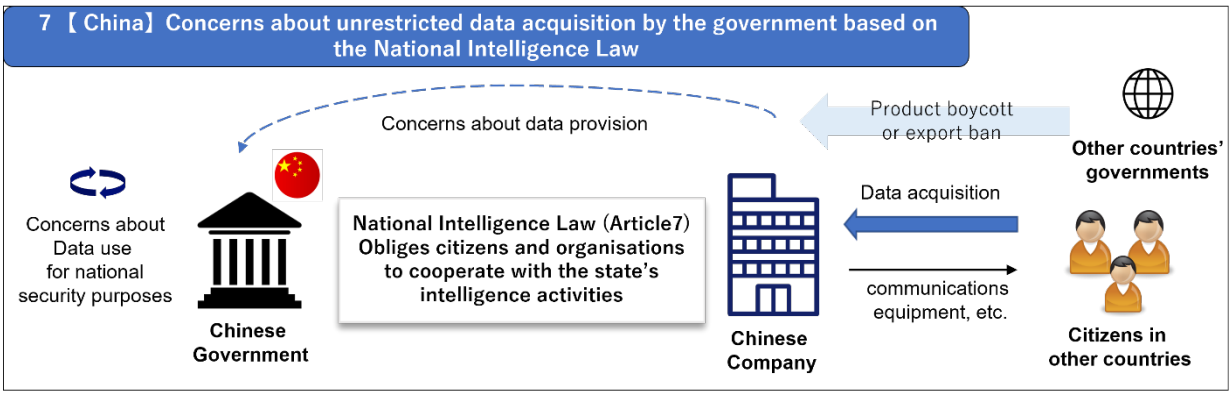
China's National Security Law, which came into force in 2015, defines national security in Article 2 as the ability to maintain a safe state of "national administration, sovereignty, unity and territorial integrity, social welfare, sustainable economic and social development and other vital interests of the country."[42]

Examining the National Intelligence Law on the premise that national security is defined broadly to include general economic development, we can imagine how Chinese companies that provide telecommunications equipment in other countries may be legally obligated to provide information and potentially forced to submit data obtained from the company's telecommunications equipment to the Chinese government without limitations. Therefore, the National Intelligence Law effectively makes it possible for the Chinese government to acquire personal and non-personal data not only from its own citizens, but also from citizens of other countries who use the products of Chinese companies. The United States, citing national security concerns, passed a bill prohibiting the certification of Chinese telecommunications equipment makers, thereby increasing their exclusion from the US market.[43]

[41] National People's Congress, "中华人民共和国国家情报法" (2018)

[42] Shikako Okamura, "China: Enactment of the National Security Law" (Foreign Legislation, No.264-2, Aug. 2015) https:dl.ndl.go.jp/view/download/digidepo_9480563_po_02640209.pdf?contentNo=1 (retrieved August 22, 2022)

[43] Taisei Toriyama, "US- and China-Made Telecommunications Equipment Exclusion Law Enacted: Huawei and others," Nihon Keizai Shimbun (November 12, 2021) https:www.nikkei.com/article/DGXZQOGN120MP0S1A111C2000000/ (retrieved August 22, 2022)



Source：Source: Shikako Okamura, "China: Enactment of the National Intelligence Law" (*Foreign Legislation*, No.272-2, 2017 August)
Taisei Toriyama, "US- and China-Made Telecommunications Equipment Exclusion Law Enacted: Huawei and others," *Nihon Keizai Shimbun* (November 12, 2021)
Figure based on source material.

Case 8 【Singapore】 Use of COVID-19 control app data for criminal investigations

The Singaporean government announced that data from a COVID-19 contact tracing app could be used for criminal investigations.

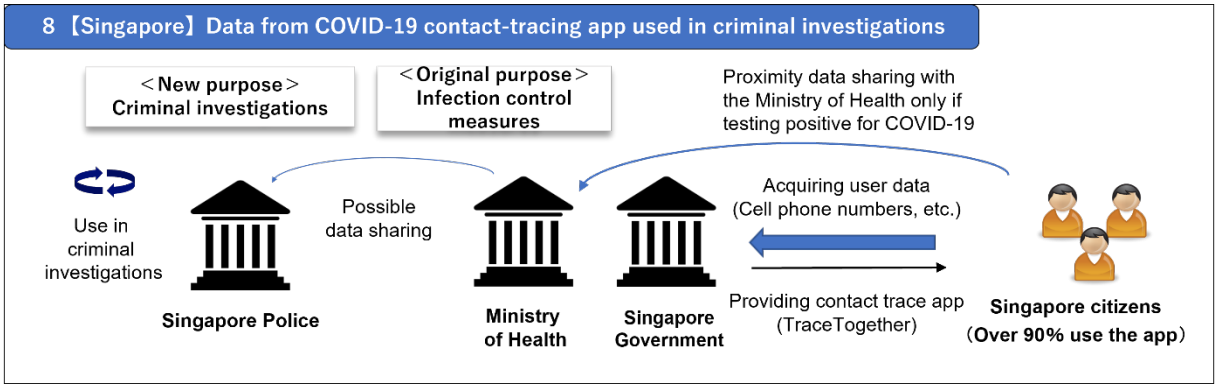
In March 2020, Singapore began using TraceTogether, a government-approved contact tracing app developed to combat the COVID-19 pandemic. As of March 2022, more than 90% of the population have downloaded this app,[44] with hotels, restaurants, shopping malls, office buildings, event venues, and many other places requiring the app for admission.[45]

TraceTogether works by exchanging anonymous IDs with proxies using Bluetooth.[46] At initial use, cell phone number and identification information are registered as user information and stored on a secure server together with randomly generated IDs. Personal location information is not collected, and a temporary ID that is updated regularly is exchanged via Bluetooth among terminals with the relevant application, located in short distance of each other. These anonymous ID data are stored on each person's device and are automatically deleted after 25 days. If a positive COVID-19 test results in a request from the Department of Health to share data, the data is manually uploaded, but if the data has not been uploaded to the Department of Health's servers, the app user may request that their identification data be deleted.

[44] Instead of downloading the app, TraceTogether Tokens (small devices) can be used.
[45] Embassy of Japan in Singapore, "COVID-19 Outbreak Alert (Part 43) (April 2021) https:www.sg.emb-japan.go.jp/files/100182789.pdf (retrieved August 22, 2022)
[46] TraceTogether Privacy Safeguards, https:www.tracetogether.gov.sg/common/privacystatement/index.html (retrieved August 22, 2022)

The app's initial privacy policy stated that "all Bluetooth data shared with the Ministry of Health will only be used for COVID-19 contact tracing." However, when a senior Singaporean government official announced in January 2021 that "the Singapore Police have the authority to obtain all data, including from TraceTogether, for criminal investigations," it was also noted that participation in contact tracing was practically compulsory. Privacy concerns drew criticism.[47] Following this announcement, TraceTogether's privacy policy was amended to add that "exceptions are made only when data are required for investigations or criminal proceedings relating to serious crimes as defined in the COVID-19 (Temporary Measures) Act."[48]

Privacy concerns have also been raised in countries other than Singapore where contact tracing apps are used.



Source：TraceTogether Privacy Safeguards, https://www.tracetogether.gov.sg/common/privacystatement/index.html, retrieved 22 August 2022.
Figure based on source material.

2. 3. Diversity of Government Access Objectives as Seen from the Case Studies

The study group decided to assume various analytical foci when analyzing government access impact based on the cases in the previous section. By doing so, it is possible to gain an overview of the reality of government access in terms of the specific objectives and what rights and interests of data subjects and the private sector are infringed upon as their data are accessed.

[47] MIT Technology Review, "Singapore Contact Tracking App Policy Shift, Made Available for Criminal Investigations" (January 2021) https:www.technologyreview.jp/s/230403/singapores-police-now-have-access-to-contact-tracing-data/ (retrieved August 22, 2022)
[48] COVID-19 (Temporary Measures) Act 2020 (No. 14 of 2020), https:sso.agc.gov.sg/Act/COVID19TMA2020?ProvIds=P111-#P111- (retrieved August 22, 2022)

It became clear that government access, including personal and non-personal data, have a broader range of objectives than access to personal data alone. In addition to law enforcement and security, which have generally been the center of discussions about government access, we confirmed that there are several examples of government access with other "public interest" objectives, such as public health (including COVID-19 countermeasures and obesity prevention), urban planning, and product safety.

Objectives of government access from the case study collection

Category	Sub-category	Relevant cases (case studies)
Law enforcement	Criminal investigations	・USA: Data disclosure from the government's criminal investigation into the Microsoft request (issue of contravening American and EU law (GDPR, etc.)) (case 6)
Security	Espionage and security activities	・USA: Forceful access of personal data transferred from the EU by the US government for the purpose of surveillance (Schrems I/II) (case 5)
	Regulating ideology and speech domestically	・Vietnam: Government censorship and deletion of content in foreign-investment SNS services (Cybersecurity Law)
Developing domestic industry	Forceful technological transfers	・China: Forceful data acquisition from foreign-owned companies and transfer to domestic industries, for example in high-tech industries (US 301-point investigation case) (case 1)
	Enhancing domestic corporate competitiveness by government-mediated data sharing	・Government support of private companies, and the building of a national voice authentication database (case 3)
Other "public" interests*	Public health	・India: Forceful acquisition of corporate health examination data and utilization for public health measures by Indian companies (non-personal data sharing framework) (case 4) ・Singapore: Government acquisition of COVID-19 app data and use in criminal investigations (case 8)
	Urban planning	・China: Real-time collection of new energy vehicle data and use in national projects
	Preventing misuse of subsidies	
	Product safety	
	Traffic safety	・China: Local government acquisition and use of operating data from technical tests related to automobiles ・EU: Building of platform to share automobile operating data between public and private actors for traffic safety (PPP)

*In a broad sense, all of the above major categories count as public interest objectives, which is why this category is named Other "public interests"

The objectives of government access also have diverse impacts on the rights and interests of governments, data subjects, and the private sector. When discussing government access centered on personal data, the protection of personal privacy and the coordination of the interests of law enforcement and security of public authorities have been key points for safeguards. In other words, if the content of the safeguard is strengthened to regulate the government's actions, personal privacy protection will be enhanced, but it is also possible that the access (government interests) will be restricted in response. The key is how to adjust the balance between the two.

However, this review positions the safeguards for government access, covering both personal and non-personal data, within a system that reconciles the diverse interests of the government that is exercising access as outlined in the table above and the rights and interests of data subjects and the private sector that may be violated by it (e.g., balancing "other 'public interests' objectives" with the data management rights and economic interests of data subjects and the private sector). This allowed us to confirm that some elements may be added to the safeguards for government access although the discussion has previously assumed the involvement of personal data.

Moreover, since governments have diverse access objectives, the types of rights and interests of data subjects and the private sector that are potentially violated have also increased. Potential concerns include not only the typical privacy rights but also intellectual property rights such as patent rights and trade secrets. Furthermore, even with government access to data that is not protected, as intellectual property rights, data subjects and the private sector are considered to have rights and interests, such as data management rights and property value. Discussions of such rights and interests are specific to big data, which are a collection of raw data not normally protected by copyrights, patents, and so forth; however, this review has shown that these rights and interests should also be protected from government access. Article 39 of the TRIPS Agreement is one basis for protecting such data collections under international rules, but the scope of application of this article is unclear and further examination is necessary.

3. Examples of previous rule discussions related to government access

In addition to the abovementioned discussions by the OECD Committee on Digital Economic Policy, we can see that there is a growing global debate about safeguards for government access. Here are some previous discussions that served as the basis of the study group's discussions.

Moreover, although details have been omitted, a "Government Access White Paper"[49] from the International Chamber of Commerce (ICC), which was still under preparation at the time of the study group's meeting and was published in April 2022, includes information exchanged during the study group's discussions.

3.1. GPA 8 principles[50]

- Purpose: Protecting privacy and promoting the rule of law
- Developed by: Global Privacy Assembly (GPA)
- Scope: Covers government access to personal data for security and public safety purposes.
- Principles: These principles are published by the GPA, which consists of data protection authorities from around the world and are sponsored by privacy authorities in Japan, France, and Canada, including the Personal Information Protection Commission. Regarding the content, the analysis is more concerned with privacy protection than with safeguards. It differs in that it stipulates, for example, the rights of data subjects in terms of right of access, correction, and erasure. See the table below for each item.

[49] ICC "ICC White Paper on Trusted Government Access to Personal Data Held by the Private Sector," April 2022.
[50] Global Privacy Assembly (GPA), "Adopted resolution on Government Access to Data, Privacy and the Rule of Law: Principles for Governmental Access to Personal Data held by the Private Sector for National Security and Public Safety Purposes," October 2021, https:globalprivacyassembly.org/wp-content/uploads/2021/10/20211025-GPA-Resolution-Government-Access-Final-Adopted_.pdf (retrieved August 22, 2022)

GPA 8 principles
1. Legal basis
Government access to personal data must be duly authorized by appropriately enacted legislation, after public debate and scrutiny by legislators. The legislation must have respect for the rights to data protection and to privacy, other human rights and be non-discriminatory.
2. Clear and precise legislation applying to government access
Any legislation authorizing access to personal information should be: a) publicly available, b) written in clear, easily understandable language, and, c) precise and specific as to the scope of personal information for which the law is granting governmental access and the conditions for such access.
3. General principle of necessity and proportionality
In order for access to personal data, including sensitive data, by state authorities or any state entity to be justifiable, the specific usage for personal information must be linked to a demonstrably necessary function or activity of government, and the intrusiveness must be proportionate to the goal in question.
4. Transparency
Any agreement or arrangement for government access, flowing from authorization in law, should also make proactive, baseline public reporting and publicly available accountability process requirements for government agencies involved, and permit information to be provided to affected individuals, unless limitations to transparency towards individuals constitute a necessary and proportionate measure in a democratic society.
5. Data subject rights
While taking into account the national security and public safety requirements, government access to personal data should integrate a specific and dedicated framework for data subjects to exercise their rights, including by addressing directly their requests to public authorities. In particular, individuals should have the right of access and to get personal data corrected or deleted, unless limitations to data subject rights constitute a necessary and proportionate measure in a democratic society.
6. Independent oversight
Laws authorizing access should consider providing for both independent advance oversight (e.g. prior judicial authorization) as well as retrospective review (e.g. auditing of

processing by independent regulatory body), taking into account the gravity and severity of the impact on fundamental rights and freedoms of individuals caused by the specific government access.
7. Statutory limitation on government's use of data acquired
Law authorizing government access to personal data for one specific purpose should regulate and frame any secondary use or onward transfer for other purposes, also observing general principles in order to ensure a continued protection of personal data.
8. Effective remedies and redress available to the individuals affected
Any governmental access to personal data should be subject to specific provisions for any individuals affected to seek effective redress and remedies.

3.2. European Business to Government (B2G) Data Sharing Principles[51]

- Purpose: To design a more flexible framework for the public sector to improve access to private sector data and its use
- Developed by: European Commission
- Scope: Covers private and government data sharing of non-personal data. The problem awareness of the European B2G (Business to Government) data sharing principles is "How should private non-personal data held by companies be used for public interest purposes by governments, and so forth?" The principles anticipate specific methods of public utilization, such as more targeted responses to epidemics, better urban planning, improved road safety and management, better environmental protection, market surveillance and consumer protection.
- Principles[52]: See the table below for each item.

[51] European Commission, "Towards a Common European Data Space," COM/2018/232 final.
[52] For the content of the principles, see the final report of the High-Level Expert Group.
European Commission, Directorate-General for Communications Networks, Content and Technology, "Towards a European Strategy on Business-to-Government Data Sharing for the Public Interest: Final Report Prepared by the High-Level Expert Group on Business-to-Government Data Sharing," Publications Office, 2021, https://data.europa.eu/doi/10.2759/731415 (retrieved August 22, 2022)

European B2G Data Sharing Principles
1. Proportionality in the use of private-sector data
Requests for the supply and use of private-sector data should be justified by clear and demonstrable public interest. The requested private-sector data should be necessary, relevant and proportionate in terms of detail (e.g. type of data, granularity, quantity, frequency of access) with regard to the intended public interest pursued. The cost and effort required for the supply and use of private sector data should be reasonable and proportionate to the public-interest benefits pursued.
2. Data-use limitation
The business-to-government collaboration agreement or the decision that requires data sharing should clearly specify the intended public-interest purpose or purposes as well as the data-use rights (e.g. stipulating what can be done with the data, time-limitation period).
3. Risk mitigation and safeguards
Private companies and civil-society organisations should not be held liable for the quality of the data in question or its use by public authorities for public-interest purposes. Business-to-government data-collaboration agreements or decisions should contain appropriate safeguards as regards the use of private-sector data in order to protect the rights (e.g. privacy, data security, non-discrimination) of stakeholders, in particular the individuals whose data is used.
4. Compensation
Business-to-government data-collaboration agreements should seek to be mutually beneficial, while acknowledging the public-interest goal by giving the public-sector body preferential treatment.
5. Non-discrimination
In business-to-government data-collaboration agreements, the private sector should treat public authorities that perform similar functions or are addressing the same public-interest purpose in a non-discriminatory way in equivalent circumstances.
6. Mitigate limitations of private-sector data
To address the potential limitations of private- sector data, including potential inherent bias, private companies and civil-society organisations should offer reasonable and proportionate support to help assess its quality for the stated purposes (e.g. type, granularity, accuracy, timeliness, format), including the possibility to verify the data,

wherever appropriate. Private companies and civil-society organisations should not be required to improve data quality at no cost.
7. Transparency and societal participation
Business-to-government data collaborations should be transparent about the parties to the collaboration and their objectives. Moreover, public bodies should ensure ex post transparency to the private companies and civil-society organisations on which particular public interest has been advanced with the use of their data and how, and cases where the data has not been used. Whenever relevant, public bodies should ensure that mechanisms are in place to stimulate public feedback and societal participation, without compromising the confidentiality of the private-sector data.
8. Accountability
All partners in a business-to-government data-sharing collaboration should be accountable for using and sharing data in a responsible and lawful way and be able to demonstrate compliance.
9. Fair and ethical data-use
Data should be shared and used in an ethical, legitimate, fair and inclusive manner, with full respect for the choices made by individuals on how their data can be used.

3.3. Japan: "Principles of Rules for Private Data Access with a High Degree of Public Interest" (Tentative)[53]

- Purpose: To expand data flow by alleviating concerns about data providers and by formulating rules that address how to motivate data providers
- Developed by: National Strategy office of Information and Communication Technology,
- Cabinet Secretariat
- Scope: Access by government agencies to private data with a high degree of public interest (the content of "highly public" is under consideration)
- Principles: See the table below for each item.

[53] Information and Communication Technology (IT) Strategy Office, Cabinet Secretariat; Intellectual Property Strategy Promotion Office, Cabinet Office, "Status of Examination of Data Handling Rules to Promote the Utilization of Data in the Private Sector", March 2021, p.18
https://www.kantei.go.jp/jp/singi/titeki2/tyousakai/kousou/2021/dai6/siryou6.pdf (retrieved August 22, 2022)

Japan: “Principles of Rules for Private Data Access with a High Degree of Public Interest” (Tentative)
1. Clarification of social significance (public interest)
Ongoing explanations of what public interest is expected and how public interest is achieved
2. Protection of privacy and intellectual property
Institutional, contractual, and technical measures necessary for the protection of privacy and intellectual property of data providers and persons involved in the generation of the data provided
3. Prevention of unintentional data flow and use
Institutional, contractual, and technical measures to prevent the unintended flow and use of data by the data provider
4. Reasonable and minimal data access
Use of data within the minimum range necessary to achieve public interest (target data, period, target person)
5. Rationality of cost burden
Cost-sharing in consideration of the investments required to generate and provide data
6. Establishment of data governance
Establishment of data governance to make 2-4 above effective (appointment of a person in charge and creating a system, formulation of data handling policies, creation and execution of human resource development plans, appropriate management and supervision of competent organizations and subcontractors, etc.)
7. Explanation of understandable and convincing data handling methods
Regarding 2-6 above, continuous explanation of understandable and convincing data handling methods and data handling situations to data providers and those involved in the generation of the data provided

3.4. Trusted Cloud Principles[54]

- Purpose: To provide the government with minimum security standards in the cloud age in order to ensure the privacy and security of customer data as a cloud operator.
- Developed by: Cloud service providers (CSPs) such as Amazon, Google, and Microsoft
- Scope: Although there is no particular limitation, since the description is based on the premise that customers can be identified, it is considered that it primarily applies to personal data subjected to government access in the possession of cloud service providers (CSPs).
- Principles: See the table below for each item.

Trusted Cloud Principles
1. Governments should engage customers first, with only narrow exceptions
Governments should seek data directly from enterprise customers rather than cloud service providers, other than in exceptional circumstances.
2. Customers should have a right to notice
Where governments seek to access customer data directly from cloud service providers, customers of those cloud service providers should have a right to advance notice of government access to their data, which only can be delayed in exceptional circumstances.
3.Cloud providers should have a right to protect customers' interests
There should be a clear process for cloud service providers to challenge government access requests for customers' data, including notifying relevant data protection authorities.
4. Governments should address conflicts of law
Governments should create mechanisms to raise and resolve conflicts with each other such that cloud service providers' legal compliance in one country does not amount to a violation of law in another.
5. Governments should support cross-border data flows
Governments should support the cross-border flow of data as an engine of innovation, efficiency, and security, and avoid data residency requirements.

[54] Amazon et al., "Trusted Cloud Principles," 2021, https://trustedcloudprinciples.com/ (retrieved August 22, 2022)

4. Discussion of government access safeguards that do not rely on personal and non-personal data

We discussed the "safeguards" required to determine the scope of appropriate government access (elements that contribute to future discussions on appropriate rule formation). The following shows the results of our analysis of safeguards related to the protection of personal information, based on the content of past discussions on that scope and adding new original interpretations (items 1 to 7, described in the text below).

The remaining items have been added as potential safeguards for government access of all types of data, without distinguishing between personal and non-personal data.

4.1. The 14 Safeguards proposed by this report

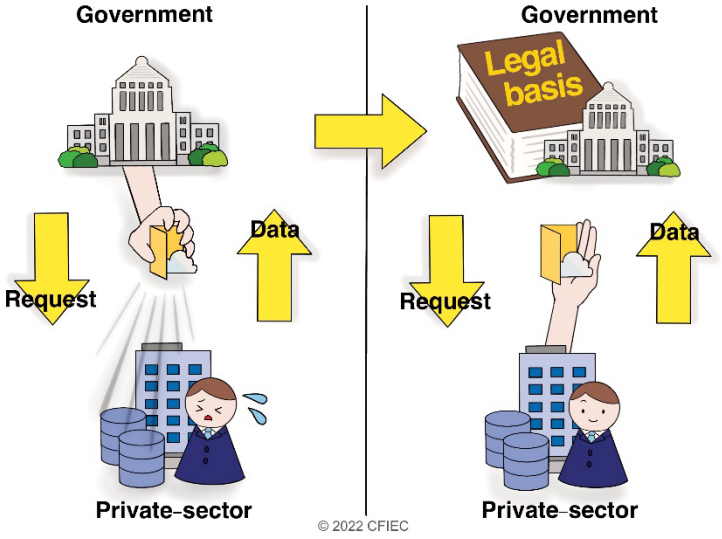
1) Legal basis

Evaluation criteria: The legal basis for enforcing government access to personal data exists on the part of the government that is providing access. Along with laws and regulations, both provisions for substantive data handling and procedures for access must be defined.

Significance and role: This provides procedures that prevent a government from exercising powers arbitrarily by clarifying legal grounds for the processing of data on the part of the government as well as improving predictability for data subjects and the private sector whose data are accessed. The absence of government safeguards can cause atrophy and impede data flow.

Relationship with other safeguards: It is anticipated that substantive content will be regulated by "necessity and proportionality" and procedural content by "approval and restriction" (both described below), which may cause some overlap with this element. However, considering that government access is permissible simply by preparing laws and regulations regardless of the content should be avoided, we also include rules concerning content in this element. Moreover, since both rules ensure predictability, there will be overlap with "transparency," but the emphasis here is placed on curbing arbitrary exercise of authority by clarifying the legal basis on the part of the government, while "transparency" is more focused on reducing the impact on data subjects and the private sector whose data are accessed.

Relationship with other international rules: The idea that procedures for compulsory treatment should be statutory is stipulated in Article 9 of the International Covenant on Civil and Political Rights (ICCPR), for example.



Legal basis

2) Meet legitimate aims and be carried out in a necessary and proportionate manner

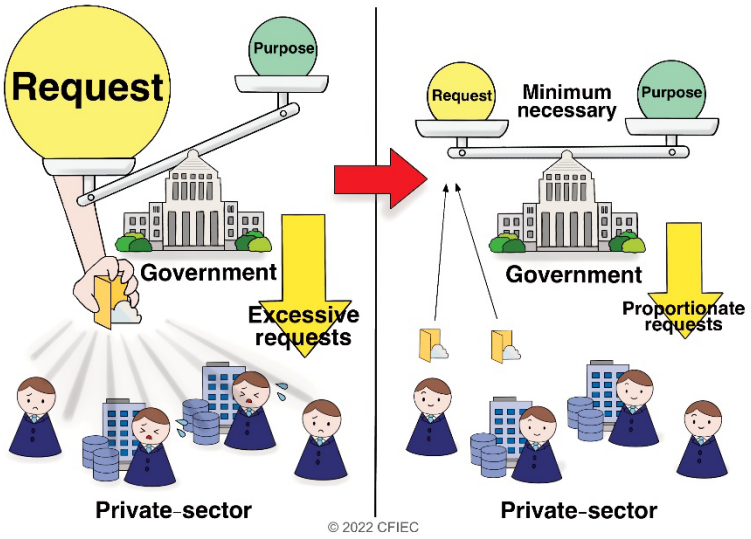
Evaluation criteria: The aims of government access need to be legitimate. The criteria for judging legitimacy can vary across political systems. Regarding the need for means, government access should contribute to the achievement of policy objectives, with no non-infringing means available other than related government access. Regarding the proportionality of ends and means, the aims and means of government access should be balanced and the outcome (or degree of infringement of rights and interests) should not be significantly disproportionate to the ends achieved.

Significance and role: This is the core element for proper government access and should ensure that the aims are not unjustified and that the legally protected interests of data subjects and the private sector are not unnecessarily infringed upon, even if there are legitimate aims. It is

necessary to limit infringement of the rights of companies and individuals to the extent necessary and reasonable to achieve the aims.

Relationship with other safeguards: The economic rationale of "the relationship between data acquisition and the realization of the aims of government access should be strictly scrutinized and rational" can be encompassed within this element.

Relationship with other international rules: The legitimacy and necessity of objectives are core elements for assessing deviations from principles in trade rules (see discussions of general exceptions in Article 20 of General Agreement on Tariffs and Trade [GATT] and Article 14 of the General Agreement on Trade in Services [GATS]).



Legitimate aims, necessary and proportionate manner

3) Transparency

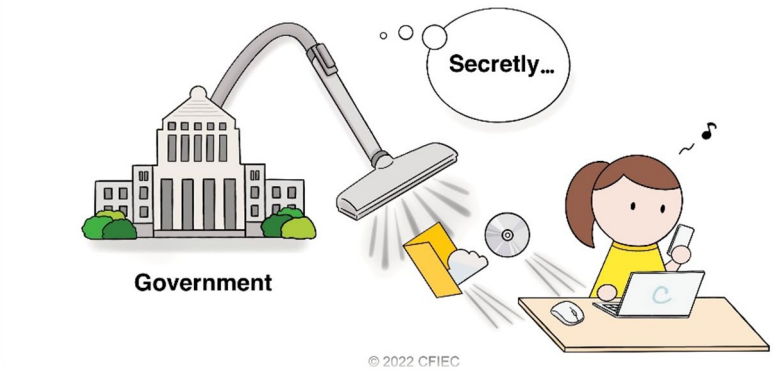
Evaluation criteria: The focus of evaluation is whether the laws and regulations that serve as the legal basis are published and available to those whose data are accessed, and whether the content is detailed enough to judge whether these safeguards are satisfied. Moreover, whether

the government is proactive in disclosing the operational status of government access (number of cases, increasing and decreasing trends, breakdown of content) and whether data subjects and the private sector, etc., are notified that government access has occurred to the extent that it does not interfere with the aims of the government access should both be considered.

Significance and role: To determine whether data subjects and the private sector whose data are accessed have received sufficient disclosure of the relevant laws and whether their content is detailed enough to evaluate whether these safeguards are satisfied, it is crucial to ensure opportunities to understand important information such as how much of your data is disclosed and what assistance you can get. Moreover, the disclosure of access information by the state allows citizens to supervise and thereby prevent abuse. Notification to data subjects and the private sector ensures that the data subjects know how their data are being accessed and offers them the opportunity to check how it matches the elements of government access and to pursue assistance regarding their rights.

Relationship to other safeguards: There is some overlap with "legal basis," but see the description under "1) legal basis" for differences. Moreover, there was initial debate about differentiating between predictability as an independent element and transparency, but we decided to integrate them into this element. Here, we consider the predictability criterion to be fulfilled if the rules are defined and published in enough detail that the data subject can access the rules and determine whether the safeguards are satisfied.

Relationship with other international rules: Article 10(1) of GATT stipulates that laws and administrative decisions, etc., "shall be immediately made public in such a manner that they may be known to governments and traders."



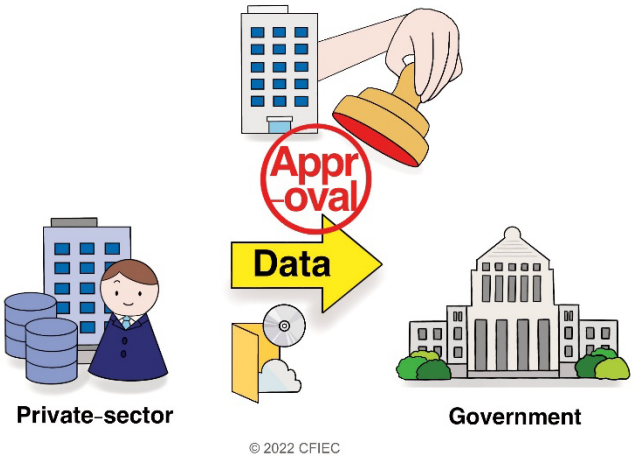
Transparency

4) Approvals and constraints

Evaluation criteria: Procedural requirements for government access are in place and the content of the procedural requirements is commensurate with the degree of infringement/intervention on the rights of individuals. In particular, when the degree of infringement is large, approval must be obtained by an independent judicial or administrative body.

Significance and role: Stipulating due process, such as the approval of government agencies and independent bodies that implement access, can meaningfully prevent infringement of companies' and individuals' rights and interest by government access that does not satisfy the safeguards. Trust can be ensured and the concerns of companies and individuals who are hesitant to submit data can be dispelled by making it clear that due process guarantees protection against infringement of rights and interests.

Relationship with other international rules: Due process is regulated by Article 9 of the ICCPR.



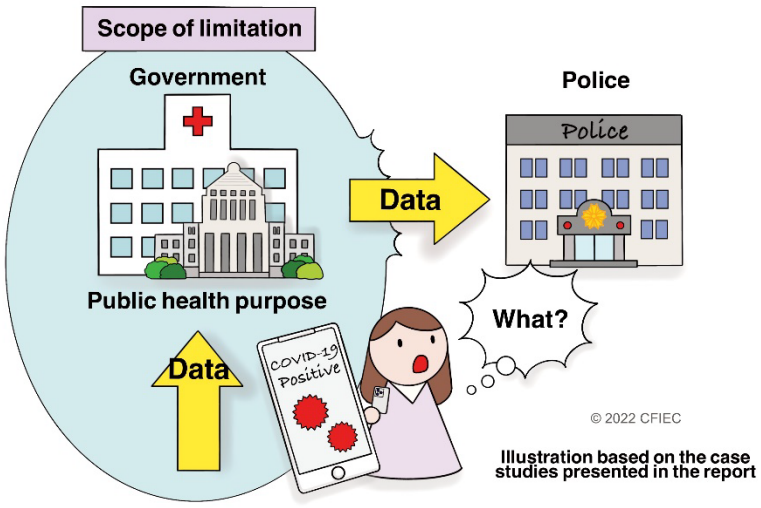
Approvals and constraints

5) Limitation

Evaluation criteria: Data accessed must be identified and handled within the confines of the relevant aims (used according to the aims). Moreover, storage of the accessed data must be evaluated in terms of the measures taken to ensure confidentiality, integrity, and useability.

Significance and role: This is to ensure that data collected through government access are used for the aims identified by approvals and constraints and are also stored with appropriate protection. The purpose of this policy is to prevent arbitrary use of data by public institutions by ensuring that the data are handled appropriately within the scope initially envisioned even after its provision, and to promote data flow by dispelling the concerns of data subjects and the private sector.

Relationship with other international rules: Principles 4 (Use Limitation) and 5 (Security Safeguards) of the OECD Guidelines on the protection of privacy stipulate related matters.



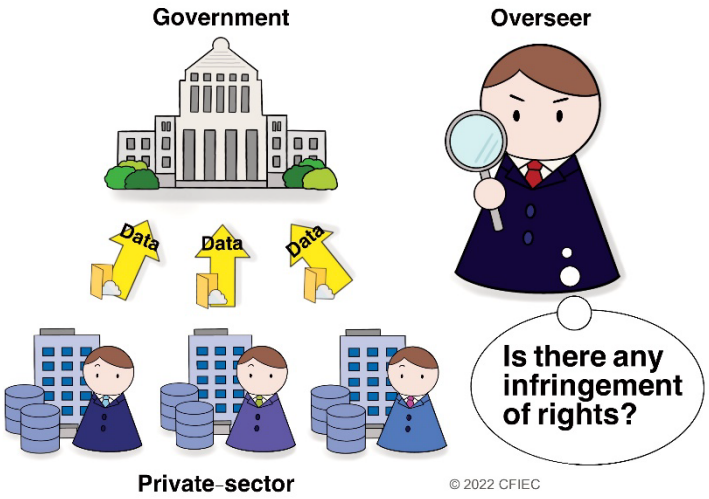
Limitation

6) Independent oversight

Evaluation criteria: Data access, use, storage, and so forth must be supervised by an independent organization after the fact.

Significance and role: Access should be supervised after the fact to evaluate whether the safeguards relevant to government access are satisfied by a body independent of the government agency implementing the access. Detecting after-the-fact infringement of the rights of data subjects and the private sector due to unjustified government access that does not satisfy the safeguards is significant because it becomes a cause for redress. By stipulating after-the-fact protection against infringement of rights and interests, trust is ensured, concerns of data subjects and the private sector are dispelled, and data flow is secured.

Relationship with other international rules: The GDPR and other regulations have provisions for supervision by independent supervisory bodies (e.g., the Data Protection Authorities [DPAs]).



Independent oversight

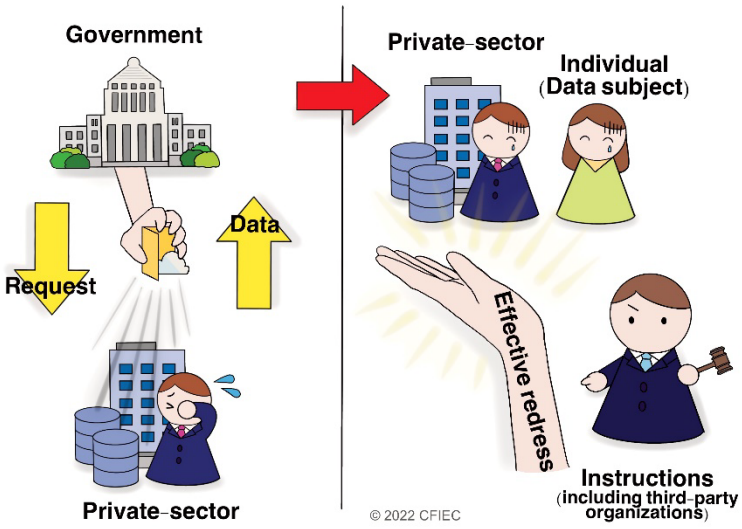
7) Effective redress

Evaluation criteria: Regarding the above rules of access, use, storage, and so forth, legally binding remedies that can be substantially employed by the data subject and the private sector in the event of a violation by the government must exist. Remedies may include damages for rights and interests.

Significance and role: This ensures that the private sector and data subjects who have been subjected to inappropriate government access are entitled to appropriate redress and compensation, such as reversal of punishments.

Relationship with other safeguards: See "12) Compensation," below, for a discussion of the relationship with "compensation."

Relationship with other international rules: Article 10(3) of GATT states that "each contracting party shall maintain, or institute as soon as practicable, judicial, arbitral or administrative tribunals or procedures for the purpose, inter alia, of the prompt review and correction of administrative action relating to customs matters." Article 14 of the ICCPR also provides for the right to a trial.



Effective redress

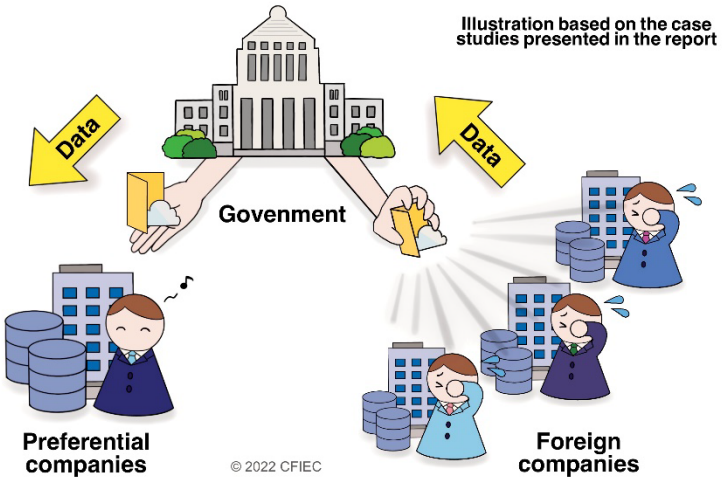
8) Impartiality and non-discrimination

Evaluation criteria: Government access must not have competitive adverse effects (competitive distortion) on the person whose data are accessed.

Significance and role: Government access is significant for ensuring equality of competitive conditions between domestic and foreign companies as well as between foreign companies in the market by not causing distortions with regards to the measure's content (structure and design of measures). If there is a competitive distortion, companies and individuals may be cut off from incentives for data collection (such as refraining from data collection or transfer for fear that their own data will flow unfairly to competitors); hence, preventing this is important.

Relationship with other safeguards: There is some overlap with "uniformity." This element focuses on the "system and results of government access," that is, the prevention of the competitive distortion effect of the structure and design of the measures themselves, or competitive distortion effects caused by the application of measures, while "uniformity" focuses on the appropriateness of the process by which measures are applied.

Relationship with other international rules: GATT and other international trade laws stipulate principles of non-discrimination (Articles 1 and 3 of GATT, etc.).



Impartiality and non-discrimination

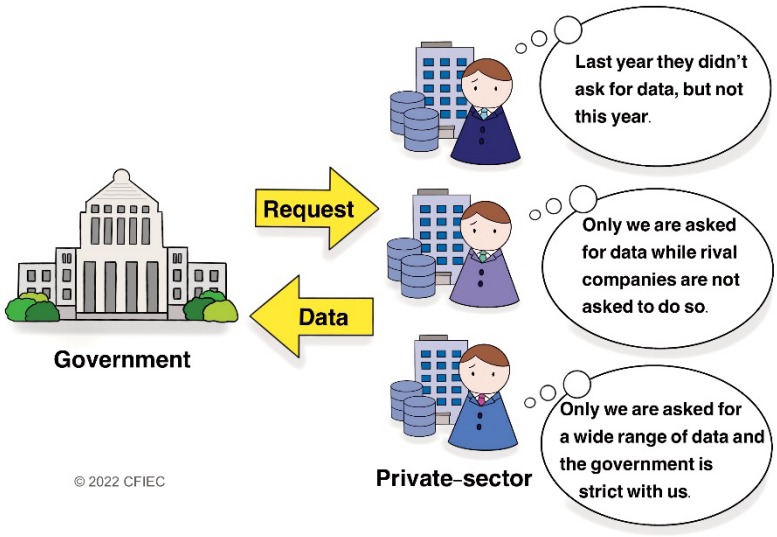
9) Uniformity

Evaluation criteria: Uniformity in the operation (process) of government access is ensured. With Article 10, Paragraph 3 of the GATT in mind, how the legal system is operated can be a criterion for determining government access.

Significance and role: Apart from whether government access has competitive distortion effects, arbitrary operation of the legal system regarding government access (non-uniform or impartial interpretation and application of the legal system, etc.) can seriously harm predictability for companies, and consequently, dampen their economic activity. In particular, if such a risk exists in a foreign market, companies will be reluctant to share or transfer data to that market, which will have a negative impact on securing international data flow. To address these issues, apart from the competitive distortion effect of government access, the need for rules to regulate the procedural appropriateness of government access was pointed out.

Relationship with other safeguards: See "8) Impartiality and non-discrimination." Moreover, in cases where the operation of the legal system regarding government access leads to different interpretations and applications depending on the company in question, but if no competitive distortion effects have occurred, this safeguard can be used rather than "impartiality and non-discrimination."

Relationship to other international rules: Article 10(3)(a) of GATT provides that "each contracting party shall administer in a uniform, impartial and reasonable manner all its laws, regulations, decisions and rulings of the kind described in paragraph 1 of this Article." The introductory clause of Article 20 of GATT also stipulates the same intent.



Uniformity

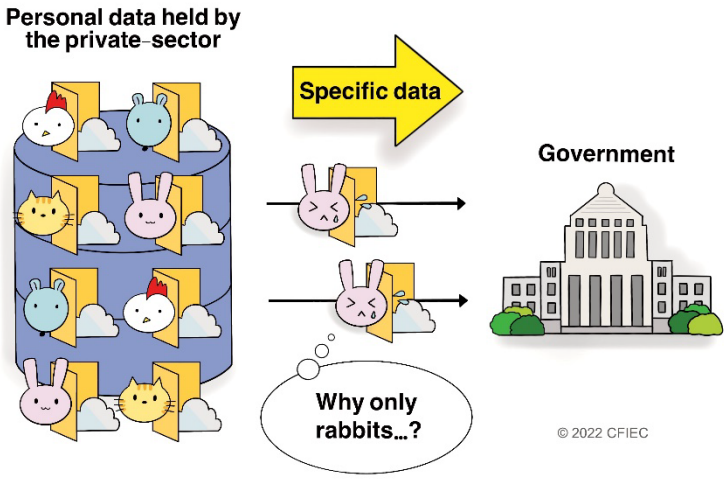
10) Fair and equitable treatment

Evaluation criteria: Treatment must not be arbitrary, unfair, unjust, or singular, and should not be based on prejudice or discrimination against race, ethnicity, culture, religion, place of residence, or gender.

Significance and role: This regulates not only anti-competitiveness, but also a wider range of factors such as prejudice and injustice. Regulating a wider range of aspects will ensure trust in how data are handled and promote data flow.

Relationship with other safeguards: Regarding the overlap with "impartiality and non-discrimination," the former focuses on anti-competitiveness, while this element is distinguished by the fact that it regulates broader aspects such as injustice and prejudice.

Relationship to other international rules: Most investment protection treaties (Article 1105 of the North American Free Trade Agreement [NAFTA]) include provisions for fair and equitable treatment.



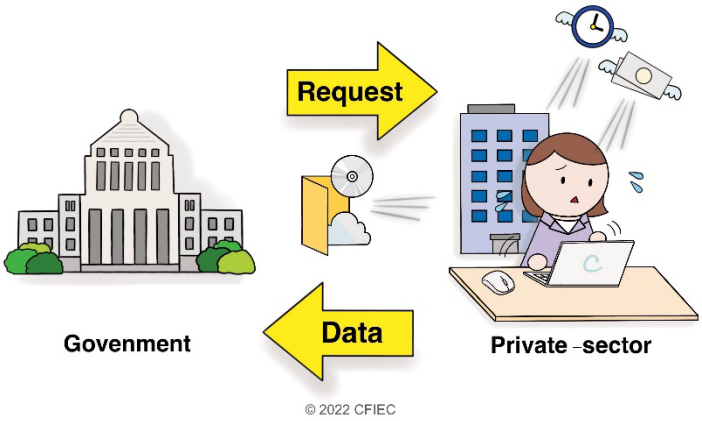
Fair and equitable treatment

11) Economic rationality

Evaluation criteria: To avoid imposing excessive costs and burdens on the private sector regarding the provision of data.

Significance and role: By not imposing excessive costs and burdens regarding the provision of data on the private sector whose data are accessed, business disruption, infringement of rights, and so forth are prevented. Moreover, by reducing the risk of being forced to bear excessive costs and burdens, this safeguard mitigates concomitant atrophic effects of data collection and transfer, thereby promoting data flow.

Relationship with other safeguards: “Compensation” and “economic rationality” are similar in that the government provides compensation when excessive burdens are imposed on the private sector and economic losses are incurred, even when government access is legal.



Economic rationality

12) Compensation

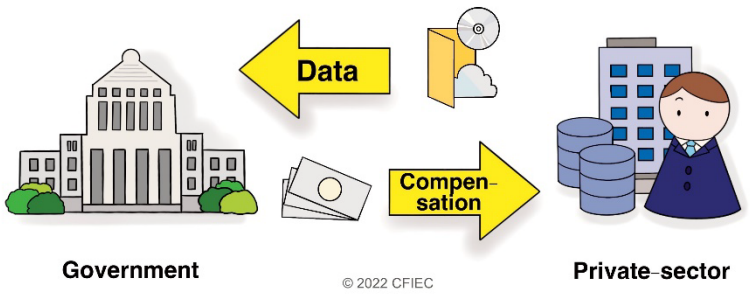
Evaluation criteria: Substantial compensation should be made to data subjects and the private sector providing data in consideration of the economic value of the data. However, compensation does not allow improper government access that is restricted by other safeguards.

Significance and role: The purpose of forcing the government to pay for the use of data with asset value is to compensate data subjects and the private sector for their interests, in the same way as property rights. Without such compensation, incentives for data collection in the countries concerned will be reduced, and competition will also be hampered by the fact that data can be used cheaply when shared among domestic companies. As a result, it becomes difficult for private sector companies to develop their businesses, and data flow itself is hindered; thus, preventing this is important. Alleviating concerns that the economic interests of private sector companies will be impaired (data that can be sold for a fee will have to be provided free of charge) is also significant. Moreover, the content of "substantial compensation" is controversial; for example, it is necessary to judge whether compensation is always required (there may be cases where compensation is not necessary), and if so, at what level (for example, market price, costs required). Such matters depend on how this term is interpreted.

Relationship with other safeguards: The relationship with "Effective redress" is as follows. "Compensation" stipulates that substantial compensation is provide even in the case of lawful

government access, while “effective redress” is supposed to compensate for damages stemming from illegal access.

Relationship with other international rules: Under customary international law, government expropriations of corporate and personal property are required to be compensated for public policy purposes, non-discriminatorily, sufficiently, effectively, and promptly. In the EU, compensation is being discussed as one of the issues of B2G data sharing as data laws are amended.



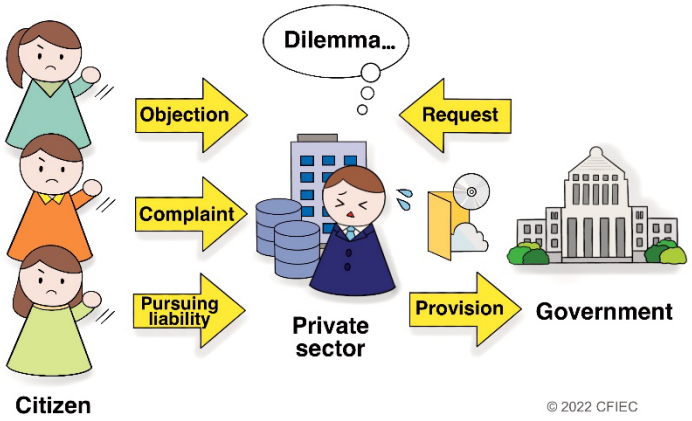
Compensation

13) Limitation of liability

Evaluation criteria: There are legal limitations of liability for the body that submits the data and the content of the data submitted (the reliability and quality of the data submitted and the limitations of liability for infringement of the data subject’s rights). However, this does not apply if the aims of the government access cannot be achieved without liability (such as providing appropriate financial information for taxation).

Significance and role: Preventing the private sector and data subjects who provide data through government access from being held unfairly liable is important. If the above unfair liability were to be imposed, the private sector would opt to not intermediate or transfer data, thus hindering data flow.

Relationship with other international rules: The EU's B2G data sharing element provides that "private companies and civil-society organizations should not be held liable for the quality of the data in question or its use by public authorities for public-interest purposes."[55]



Limitation of liability

14) Conflicts of law

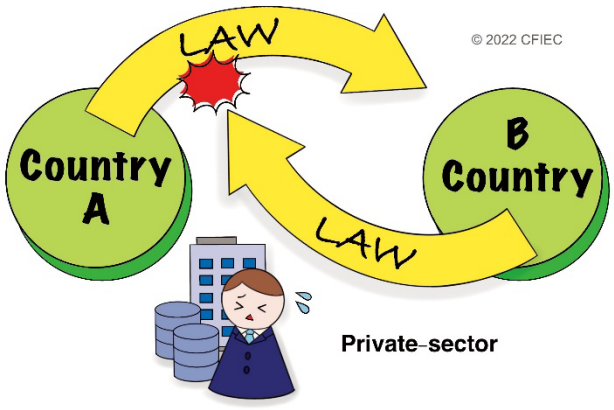
Evaluation criteria: To address conflicts of law arising from government access (inconsistencies with other legal systems), ensure that compliance with laws and regulations in the country where government access is implemented does not violate the laws and regulations of that or other countries. Mechanisms to address and resolve contradictions and conflicts in domestic and foreign legal systems should be established.

Significance and role: In the event of a conflict between the legal obligation to provide data via government access and the legal obligation to prohibit data provision to a third party in another

[55] European Commission, Directorate-General for Communications Networks, Content and Technology, "Towards a European strategy on business-to-government data sharing for the public interest: final report prepared by the High-Level Expert Group on Business-to-Government Data Sharing," Publications Office, 2021, p82, c), https://data.europa.eu/doi/10.2759/731415 (retrieved August 22, 2022)

country, reducing the burden on the private sector by making adjustments in advance is necessary. If there is a legal system that causes such a conflict of law to occur, that risk of conflict might cause business restrictions as the private companies hesitate to enter the market and business development is hindered. The private companies could then be motivated to change the location of their servers or abandon business development to avoid risk. This hinders data flow.

Relationship with other international rules: Article 31 (International access and transfer) of the EU Data Governance Act provides that public authorities, private companies, and individuals should take all possible technical, legal, and organizational measures to avoid cross-border transfers of data so as to avoid conflict with laws in the EU or its member states. Here, it is stipulated that data may be transferred based on the request of a foreign government and so forth in exceptional cases where certain conditions are met, such as when there is a mutual legal assistance treaty or when appropriate protection is provided in that foreign country.



Conflicts of law

4. 2. Organizing Inter-Element Relations

We have organized the above 14 safeguards to avoid excluding the possibility of overlapping meanings or that one safeguard could be included in another, while attempting to depict the

overall picture of the required rules in their entirety. As such, the analysis is described safeguard by safeguard, paying attention to the relationships between the safeguards and the individual concepts that appear in their descriptions, and then describing the relationships between the safeguards and concepts of particular note.

1) The meaning of proportionality

Since there may be multiple understandings of what "proportionality" means, we would like to go over the term here. "Proportionality" is mentioned as a secondary element in the 2020 CDEP statement, with no description of what it refers to. On the other hand, it is considered one of the core elements of the government access safeguards in the GPA 8 Principles, along with necessity. Based on the belief that proportionality is an important safeguard for government access, we decided to explicitly address it as one of the safeguards.

Although it has been pointed out that the principle of proportionality is a concept specific to EU law, the proportionality described in these rules is similar to Japan's interpretation of its constitution. Since this is a more general concept, we decided to include it as a safeguard.

2) The relationship between compensation and redress

An overlap between the safeguards for compensation and redress has also been pointed out. Here, redress assumes the ability of the data subjects and the private sector to stop an infringement or receive compensation for damage suffered due to infringement of rights and interests from government access that does not comply with the safeguards.

On the other hand, compensation does not necessarily assume a violation of the rules, but even if it is lawful government access, reasonable compensation should be given based on the data's economic value when provided by the private sector subjected to government access. The focus here is on the economic value of the data, which is a safeguard that has been newly identified in this review. However, compensation is not always required, making it different from redress.

3) The relationship between impartiality, fairness, and being fair and equitable

The question also arises as to whether impartiality and fairness should be distinguished from each other. While impartiality is an economic concept centered on the prevention of distortion of competition, fairness is concerned with a broader range of rules and norms, such as discrimination, human rights, and injustice; hence, the two should be distinguished.

It was also mentioned that fairness in particular is ambiguous depending on the context and time period. This makes it insufficiently solid as a safeguard, but we still decided to adopt this term as the words fair and equitable are used in international rules as a concrete definition of fairness.

5. Summary of Study Results and Future Perspective

5. 1. Characteristics of the Rules Required for Non-Personal Data

Compared to cases concerning personal data, the safeguards that cover non-personal data incorporate the complex relationship between the objectives of government access and the interests of data subjects and the private sector whose data are accessed. Consequently, it was necessary to consider various cases regarding how closely the two should be coordinated. There are points of contention about the extent to which it is appropriate to assess the need for government access and seek alternatives, and whether the examination criteria for the government access safeguards should be uniform for various cases. When it comes to "other 'public interest' objectives" (see table in 2.3.), data are used for the benefit of maintaining the safety of citizens and the world as a whole (e.g., pandemic response). In terms of system design, it is important to consider the reasons that will determine when data should be provided to increase the overall benefit to society. It was also suggested that the concept of institutional design may be different from that of security, such as law enforcement and counterterrorism.

The criteria for judging the legitimacy of the aims were also a point of contention. Although it is related to the point that "Assuming a standpoint of global rulemaking, our consideration policy was aimed at formulating rules so that specific states (for example, countries with certain political systems) would not be uniformly excluded," described in Chapter 1 (1.2.), there is also

a connection to the question of whether government access used to sustain certain political systems (e.g., a dictatorship) should be considered a legitimate aim.

Further examination of the above two points will be necessary in terms of the understanding of government access and changes in examination criteria based on it. In international trade agreements, there are prescription methods for changing examination criteria by enumerating policy objectives in a limited way (GATT and GATS types), as well as prescription methods that abstractly prescribe only the legitimacy of policy objectives and uniformly prescribe examination criteria (exceptions to Chapter 14, Electronic Commerce of the Trans-Pacific Partnership (TPP), etc.). Thus, the manner in which safeguards for government access are prescribed may also depend on the prescription method used for the trade rules that they are part of. It should also be noted that security exceptions are separately established for both prescription methods.

While personal data is considered more important than non-personal data in international negotiations, the inclusion of non-personal data in this report adds new safeguards.

As for relations with China, how to deal with the "National Intelligence Law" is a major issue, for which future discussions are necessary. The cases analyzed here are limited to those that involve enforcement in some way; thus, the ideas behind the safeguards described here are also limited. As an example, which we were unable to examine at this time, there is a case where Yahoo! JAPAN received a request by the government to provide voluntary data as part of COVID-19 countermeasures, and concluded a contract concerning voluntary provision. Since such cases are expected to increase in the future as part of the governments' use of data, it is necessary to consider safeguards for government access, including situations where the private sector voluntarily provides data to the government.

Regarding economic security, a discussion may be necessary regarding a bill that would prescribe government access authority in Japan. While it is important to protect the rights and interests of Japanese data subjects and the private sector from foreign government access, it needs to be assumed that safeguards apply not only to the country/region of concern, but also to own country and friendly countries. It would be hoped by the private sector that the scope of appropriate compensation would not be limited to those envisaged for personal data but would also take account of damage caused to small and medium-sized enterprises.

5. 2. Issues Concerning the Application of Government Access Rules to Trade Rules

When government access is considered as an issue under trade rules, it requires different considerations from the discussion around personal data in several respects.

The first issue regards what countermeasures are permissible against countries that do not seem to comply with safeguards for government access. To take an extreme example, the countermeasure would be to deny data transfers from that country (prohibition of cross-border data transfers), as well as providing special security control measures to transfer destinations in that country (for example, the SCC response based on the Schrems II verdict under the GDPR), and to specify government access risks by that country when acquiring consent (the 2020 revision of the Act on the Protection of Personal Information in Japan). Continued consideration is required to ensure that reciprocity is assumed but does not undermine the claim of free cross-border data flows.

Second, it is necessary to proceed with the reorganization of the relationships with existing trade rules. It is effective to clarify to what extent government access can be managed through existing trade rules such as the TRIPS Agreement, which will reveal holes in the rules and clarify the necessity of establishing new safeguards for government access.

Third, we should also consider conflicts between government access rules and existing trade rules. For example, prohibiting cross-border transfers of data to countries that do not seem to comply with government access safeguards, cited as an example above, could be a violation of a provision of the TPP Agreement (Chapter 14, Electronic Commerce).[56] Moreover, market distortions of fairness are partly covered by WTO subsidy agreements and the GATT/GATS principle of non-discrimination, but it is necessary to sort out the relationships, such as overlapping coverage and contradictions.

5. 3. Toward Future Rule Formation

This report summarizes various ideas about safeguards for government access rules as a basic study for the formulation of trade rules.

[56] However, the TPP Agreement (Chapter 14, Electronic Commerce) is necessary to achieve legitimate public policy objectives that are exceptional, and since limitations on data transfers can be allowed in exceptional cases when certain conditions are met, in the absence of arbitrary or improper discrimination, we find that this relationship, with exceptions, is necessary.

It is expected that this examination of safeguards for government access will continue in the future. It is possible that discussions will be held at various forums such as the OECD, where it is already underway, and G20, as well as at G7 and the Internet Governance Forum (IGF), both of which will be held in Japan in 2023. We hope that Japanese policymakers, corporate practitioners, and experts from other countries will refer to it in rulemaking. In addition, the evidence required for rulemaking is important, and it is expected that the economic and other impacts of government access will be collected and analyzed in the future, and then build further discussions on that basis.

We assume that it will take some time to formulate the global rules for government access; however, the measures we discussed included suggestions that can be regulated using existing domestic laws and international trade agreements. For example, requests for disclosure of confidential technical information in exchange for administrative approval in case 1 include the pharmaceutical production industry, and drug test data is protected by Article 39 (3) of the TRIPS Agreement. In addition, the Brazilian Parliament has debated the appropriateness of forcing pharmaceutical companies to share information, including the expertise they possess. This is an example of government access that may violate that same article.

On the other hand, it is also important to consider how existing national and international rules can be utilized. There is also room to consider the feasibility of utilizing FTAs and investment protection agreements. By accumulating examples of dispute resolution related to existing international rules, it is possible for Japan to take the lead in forming a certain market view on how to interpret international agreements. This will encourage rulemaking through dispute resolution and complement new rules that require international agreement.

In the private sector, in-house experts are examining the appropriateness of government access in response to facing such access, but there is a need for rules that can be used as a reference for this. The safeguards proposed here can serve as these sorts of references, but as they are abstractly expressed, guidelines are also needed to bridge the gap with corporate practices.

For the protection of non-personal data, there are matters for which global rules have not been established. One example is the collection of so-called big data, a large amount of data that is accumulated for AI algorithms and data analysis. This is not protected under copyright because it is not original, and applications for patents and such are seldom filed; moreover, these collections are often not protected as business secrets either.

International debate continues about whether data that are not protected as intellectual property rights should be protected, and what rights apply if they are protected (the debate about data ownership under the EU Data Act, limited provision data in Japan, etc.). The concept of protection of rights and interests is important when considering the safeguards for non-personal data. It is necessary to continue to pay close attention to how these debates unfold and to incorporate that into our discussions about safeguards for government access.