Nishimura Institute of Advanced Legal Studies ("NIALS")

Report by the

CLOUD Act Study Group

Ver. 2.0

Legal Analysis and Proposals On Criminal Investigations Obtaining Data Held by Companies

NISHIMURA & ASAHI

This is an English translation of the Japanese original released by NIALS in April 2023.

Ver. 2.0: April 2023
Ver. 1.0: December 2019

Nishimura Institute of Advanced Legal Studies

Participants (names listed without honorifics) of the CLOUD Act Study Group ("Study Group"), NIALS:

<<Chairperson>>

George Shishido, Professor, The University of Tokyo Graduate Schools for Law and Politics

<<Members>>

Yurika Ishii, Associate Professor, Department of International Relations, National Defense Academy, Ministry of Defense of Japan
Go Naruse, Associate Professor, The University of Tokyo Graduate Schools for Law and Politics

<<Secretariat>>

(As of April 2023)
Nishimura & Asahi:
Kojiro Fujii, Attorney-at-law
Takayoshi Hojo, Attorney-at-law
Shimpei Ishido, Attorney-at-law
Taku Nemoto, Attorney-at-law
Tatsuya Tsunoda, Attorney-at-law
Shunya Muromachi, Attorney-at-law
Hanako Ohwada, Attorney-at-law
Kei Ogawa, Attorney-at-law

(As of December 2019)
Nishimura & Asahi:
Kojiro Fujii, Attorney-at-law
Takayoshi Hojo, Attorney-at-law
Shimpei Ishido, Attorney-at-law
Makiko Tsuda, Attorney-at-law
Tatsuya Tsunoda, Attorney-at-law
Marie Wako, Attorney-at-law
Atsushi Kono, Attorney-at-law
Yusuke Iwaya, Attorney-at-law
Hibiki Kimura, Attorney-at-law
Shunya Muromachi, Attorney-at-law

<<Supporting Companies with respect to presentations, hearings, etc.>>

The Study Group's hearings and other efforts were supported by the following domestic and overseas communications and IT companies and organizations before the release of Ver. 1.0 of this report:

NTT Communications Corporation
Twitter Japan, Inc.
Microsoft Japan Co., Ltd.
Mercari, Inc.
Yahoo Japan Corporation
LINE Corporation
The American Chamber of Commerce in Japan
and two other companies

*The body of this report, including proposals by the Study Group, represents the views of the lawyers of Nishimura and Asahi participating in the Study Group and does not reflect the views of the Chairperson, the Members of the Study Group, or the Supporting Companies.

Table of Contents

I. Purpose of the Study Group and Structure of This Report

On March 23, 2018, the Clarifying Lawful Overseas Use of Data Act (the "**CLOUD Act**"), which clarifies procedures in the United States when an investigating authority issues an order to disclose data that a company stores on servers located outside of the U.S.,[1] was enacted. In connection with this, NIALS held a symposium on the CLOUD Act on March 13, 2019 to increase awareness about issues concerning the CLOUD Act among the industrial, governmental, and academic sectors in Japan.

In addition, NIALS established a Study Group, which seeks to analyze and make proposals regarding Japan's response to the CLOUD Act, to begin, as well as more broadly regarding issues relating to obtaining data held by companies for criminal investigations under Japanese law and international law, as well as from the perspective of international and public-private cooperation. The Study Group consists of legal scholars, and was managed by the lawyers of Nishimura & Asahi, who served as the secretariat. In the course of discussions, the Study Group also obtained input from a substantial number of domestic and foreign Internet companies and data companies. The results of the Study Group's discussions were summarized in this report in December 2019.

Thereafter, the Supreme Court of Japan rendered a decision on cross-border remote access (Supreme Court, Decision dated February 1, 2021, Keishu [*Supreme Court Criminal Case Report*] vol. 75, no. 2, p. 123) (the "**2021 Supreme Court Decision**"), and progress was made in discussions concerning the introduction of IT in criminal proceedings. Internationally, in addition to the Second Additional Protocol to the Convention on Cybercrime, there were also developments in the discussions concerning executive agreements based on the CLOUD Act, EU regulations on the collection of electronic evidence, discussions on the government access in the Organization for Economic Cooperation and Development (the "**OECD**"), and other related topics. Based on the developments in these areas, the Study Group updated this report in April 2023.

The structure of this report is as follows. Part **II** outlines the proposals of the Study Group contained in this report. Next, Part **III** gives an outline, and explains the significance, of the CLOUD Act, which raised questions about obtaining data held overseas by companies, as well as the proposed EU Electronic Evidence Regulation and Directive, which aim to establish a comprehensive legal framework for obtaining electronic evidence. Based on these international movements, Part **IV** explores the issues relating to investigative methods for obtaining data held by companies under Japanese law, and Part **V** analyzes the issues that arise, particularly, where data held by companies may be stored abroad. Part **VI** then presents the Study Group's suggestions for international collaboration regarding investigative methods for obtaining data held by companies, including a suggestion for the Japanese government to enter into an executive agreement with the U.S. government, which will resolve these issues. Part **VII** addresses the actual responses from domestic and foreign companies to requests seeking data for investigative purposes in light of the issues mentioned and the actual circumstances the companies face, and also touches upon the future outlook. Finally, Part **VIII** touches on the implications and influences that analysis and discussion of the issues concerning investigative methods for obtaining data held by companies could have on policies for the free flow of data. The main laws, regulations, treaties, conventions, and the like referred to in this report are attached to the end of this report as reference material (**Reference Material: Collection of Relevant Provisions (as of April 2023)**).

We hope that, going forward, the Study Group's proposals and supporting legal analyses, will be helpful for discussions on laws and policies in Japan and on creation of an international framework regarding data held by companies and investigations.

---

[1] In this report, data stored on servers over which a company has managing authority is described as "data held by a company," and data stored on servers located in a foreign country is described as "data stored in a foreign country." For the meaning of "manage," *see* footnote 48 below.

II. The Study Group's Proposals

In recent years, data accumulation in companies has progressed and active cross-border data transfer has taken place more frequently. In these circumstances, there have been many cases where a crime is committed in Japan, and data which is important evidence in the subsequent criminal investigation is held by a company on servers located in foreign countries. In order for Japanese investigating authorities to effectively obtain data necessary for investigations, and for the Japanese criminal laws and regulations to be appropriately and expeditiously applied, it is increasingly important not only to obtain data stored on the terminals of suspects, but also to obtain data held by companies in Japan and in foreign countries.

However, the design of a systems for investigative methods for obtaining data held by companies in Japan and in foreign countries is still in a developmental phase, and it is necessary to consider various issues, including those mentioned below, in designing this system; however, these issues are not fully analyzed.

In other words, in situations where data held by companies is to be obtained for investigative purposes, it is also necessary to guarantee the rights and interests of the person(s) to whom the content of the data relates ("**Data Subject**"),[2] to take into account the burden on domestic and foreign companies holding the data, and to obtain the understanding of civil society. Furthermore, since electronic data can easily be modified, deleted, and concealed by encryption or other means, it is also necessary to consider how to secure the effectiveness of investigations bearing in mind such characteristics of electronic data. Also, where there is a possibility that electronic data held by a company is stored abroad, it is necessary to consider how to ensure conformity with international law and international collaboration.

Based on the issues and circumstances described above, in this report, NIALS analyzes the discussions on each issue and makes the following proposals:

1. Further Use of Existing Investigative Methods for Obtaining Data Held by Companies, and Considering New Systemic Designs

- ✓ In recent years, data accumulation in companies has progressed, and it is necessary for investigating authorities to obtain data held by companies efficiently and effectively through cooperation with companies, while taking into account the interests of Data Subjects and companies. A system exists under current laws for seizure via an order to produce a copy of records, to ensure this cooperation, and it is expected that this system will be used actively; however, there are also issues with this system. Under these circumstances, the Criminal Law (pertinent to information and communications technologies) Subcommittee of the Legislative Council of the Ministry of Justice currently is holding discussions to promote digitized or online warrant proceedings and to establish a system for Orders to Produce Electromagnetic Records. If these goals are realized, it is highly expected to promote efficient, effective data acquisition through smooth cooperation between investigating authorities and companies. There are various issues to consider when designing these systems, such as ensuring security when presenting an online warrant to a company holding data, and when submitting data, ensuring the fairness and transparency of procedures for prior or subsequent notice to Data Subjects, expansion of the system to impose confidentiality obligations and similar restrictions, and analyzing relationships with other laws and regulations

---

[2] When using the term "person" in relation to a principal to whom the contents of data is related, this term typically refers to a subject that is assumed to fall within the definition of "person" in Article 2, paragraph (4) of the Act on the Protection of Personal Information.

relating to data protection. It is necessary to advance discussions on these issues while considering technological innovations and sophisticated criminal investigations, domestic and foreign companies' response policies and actual responses, and movements in foreign countries and international forums, with the aim of strengthening both investigating authorities' investigative capabilities and protecting the rights of relevant persons. (**IV.1** below)

- ✓ Another method for investigating authorities to obtain data held by companies is to access the server, where the data is stored, by themselves (i.e. remote access). While this investigative method is useful in different ways from the method of asking companies to submit data, it is advisable to examine the design of the system further, to give consideration to the interests of Data Subjects and the companies that are server-managing entities, as well to guarantee due process of law in the future. (**IV.1** below)

- ✓ In addition, the prospect of the data so obtained being used in a criminal trial should be considered. In this respect, the relevant Subcommittee of the Legislative Council of the Ministry of Justice has considered the examination methods for trials where data is presented as evidence; however, moving forward, it is advisable to establish certain objective indices (standards or criteria) in order for courts to appropriately evaluate the authenticity and probative value of the data presented as evidence (**IV.2** below).

2. Deepening Discussions Regarding Trans-border Data Access for Investigative Purposes From the Perspectives of International Law, and Participating in the Establishment of a Cross-national Framework

- ✓ There are ongoing domestic and international discussions regarding the legality of obtaining data stored outside the territory of an investigating authority. Under international law, if a state exercises its jurisdiction in the territory of another state, such an act infringes upon the other state's sovereignty. However, it is also possible to conclude that obtaining data stored on servers located in the territory of another state for investigative purposes, for example, through the issuance of a data production order against a domestic company with regard to its data stored overseas, does not necessarily constitute an unlawful exercise of the investigating country's jurisdiction in the territory of another state, depending on the method employed. In Japan, the 2021 Supreme Court Decision triggered discussions on the methods and limits of trans-border data access; however, given the importance of obtaining data stored abroad appropriately and swiftly, Japan should endeavor to deepen discussions of investigative methods that accord with international law while maintaining Japan's policy of respecting the sovereignty of other states (**V.1** below).

- ✓ In addition to building multinational frameworks, such as the Convention on Cybercrime and the Second Additional Protocol, international collaboration can be achieved and advanced through the establishment of bilateral (or multinational) frameworks as envisioned by executive agreements pursuant to the CLOUD Act. As a first step, it is considered effective for Japan to build this type of bilateral (or multinational) framework with like-minded countries with which Japan shares internationally recognized principles, for example, the OECD Government Access Declaration concerning access by public bodies to data held by companies (government access) (**Column (i)** below), and a common sense of values, in accordance with the trustworthy concept of Data Free Flow with Trust ("**DFFT**"), while also participating in discussions toward building a multinational framework. If development of a system for Orders to Produce Electromagnetic Records, or other systems, progresses in Japan (*see* Proposal **1**), this will lead to establishment of a

foundational system that will allow for bilateral (or multinational) collaboration with like-minded countries, including the U.S.; therefore, it is advisable to proceed with necessary discussions on legal issues to execute bilateral international agreements with like-minded countries (**V.2**, **VI**, and **VIII** below).

3. Promoting Companies' Efforts to Ensure Transparency of Government Access

- ✓ In order to obtain a deeper understanding from Data Subjects and civil society regarding obtainment of data held by companies for investigative purposes, in addition to government-level efforts, it is important that companies and industries also make voluntary efforts to ensure transparency regarding government access, such as releasing transparency reports that aggregate responses to requests for government access, and preparing and releasing response policies. (**VII** below)

- ✓ These efforts will allow companies to provide a sense of security to users who are Data Subjects and to improve civil society's trust in each company, and will contribute to the competitiveness and interests of companies in the long run. Therefore, companies and industries are also expected to advance discussions on specific efforts to ensure the transparency of government access (disclosing response policies and actual responses to investigating authorities' requests for disclosure of information) and to make increased efforts in this regard (**VII** below).

III. Developments in the U.S. and EU

1. U.S. CLOUD Act

(1) Background to Enactment

In the U.S., before the enactment of the CLOUD Act, no laws or regulations contained provisions that explicitly authorized U.S. government bodies to issue an order for the submission of data stored outside of the U.S., including the Stored Communications Act (the "**SCA**") which provided procedures for U.S. government bodies to request disclosure of data retained, stored, or controlled by electronic communications service providers or remote computing service providers. However, although the U.S. government was able to obtain data stored outside of the U.S. pursuant to the procedures established by Mutual Legal Assistance Treaties ("**MLAT**" or, in the plural, "**MLATs**"), their efficiency and certainty were questioned, and the extraterritorial application of the SCA was being debated.

Against this backdrop, when a U.S. investigating authority requested Microsoft Corporation to disclose data stored on its servers located in Ireland under the SCA without using the MLAT, Microsoft Corporation refused the request for the reason that the servers were located outside of the U.S. and moved to quash the warrant. Although the federal district court denied the motion, upon Microsoft's subsequent appeal, the Second Circuit Court of Appeals rejected the extraterritorial application of the SCA and upheld Microsoft's appeal.[3] Against this background, voices seeking clarification of the laws and regulations governing the ability to obtain data across borders for investigative purposes became louder, which led to the enactment of the CLOUD Act.[4]

(2) Overview of the CLOUD Act

The CLOUD Act was enacted on March 23, 2018, as a part (DIVISION V) of the Consolidated Appropriations Act of 2018. The two main features of the CLOUD Act are set forth below.

First, the CLOUD Act clarified the authority of U.S. government bodies to compel a provider subject to U.S. jurisdiction[5] to store, back-up, and disclose data held outside of the U.S. pursuant to a warrant or similar enforceable instrument under the SCA.[6] However, a provider who is required to disclose data may file a motion with a U.S. court to modify or quash the disclosure order where the provider reasonably believes that (i) the Data Subject is not a U.S. person and does not reside in the U.S., and (ii) the required disclosure would create a material risk that the provider would violate the laws of a foreign government with which the U.S. government has entered into an executive agreement (*see* **VI** below); whether to modify or quash the order is decided via comity analysis, based on statutory elements to be considered.[7] In addition, even if requirements (i) and (ii) are not met, the provider

---

3 *U.S. v. Microsoft Corp.*, 829 F.3d 197, 200-201 (2nd Cir. 2018) (the "**Microsoft Case**").

4 Due to the enactment of the CLOUD Act, the Supreme Court caused the Microsoft Case to be terminated for the reason that the necessity to make a decision ceased to exist (*U.S. v. Microsoft Corp.*, 138 S. Ct. 1186 (2018)).

5 The U.S. government clearly states that U.S.-based business operators are typically assumed to be providers that are subject to U.S. jurisdiction, but that non U.S.-based business operators that provide services in the U.S. may also be subject to U.S. jurisdiction in some cases (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*, p. 8 (Apr. 2019), *available at* https://www.justice.gov/opa/press-release/file/1153446/download).

6 CLOUD Act Sec.103(a)(1), 18 U.S.C. Sec. 2713.

7 CLOUD Act Sec.103(b), 18 U.S.C. Sec. 2703(h).

may also contest the disclosure order before the courts based on the concept of comity,[8] as an international legal principle, on the basis that the provider would violate the laws of a foreign government if it provided the data.[9]

Second, the CLOUD Act establishes that where the U.S. government and a foreign government have entered into an executive agreement, if a provider subject to U.S. jurisdiction discloses data in response to a foreign government's direct order, such disclosure will not be deemed illegal under U.S. laws, such as the Wiretap Act.[10] As a result, U.S. providers can directly respond to a foreign government's orders, and the foreign government can expeditiously receive the submission of data stored outside of the country by means other than MLATs. However, in order for a foreign government to enter into an executive agreement with the U.S. government, the U.S. Attorney General's certification is required with regard to whether the foreign government affords robust substantive and procedural protections for human rights (for example, privacy and freedom of expression) and has adopted appropriate procedures to minimize the acquisition, retention, and dissemination of information concerning U.S. persons.[11] Since an executive agreement is based on the principle of reciprocity, companies of a country which has entered into an executive agreement with the U.S. must respond to the U.S. government's orders.[12]

Several companies have welcomed the introduction of the CLOUD Act because it clarifies the law regarding data disclosure orders.[13] On the other hand, some U.S. human rights organizations point out that the legislative process for the CLOUD Act was rushed and have expressed concern that the negotiation process for entering into an execution agreement is unclear.[14]

In April 2019, the U.S. government released a white paper regarding the CLOUD Act,[15] stating that the U.S. government expected that the CLOUD Act and executive agreements, together, would establish legal provisions on obtaining data stored in other countries for investigative purposes. In fact, the U.S. government entered into an executive agreement with the U.K. on October 3, 2019,

---

8 "Comity" refers to situations where a court makes a decision by respecting a decision of a foreign country on the basis of friendship, etc., as opposed to doing so as a matter of right (Hideo Tanaka ed., *DICTIONARY OF ANGLO-AMERICAN LAW*, p. 161 (University of Tokyo Press, 1991)).

9 CLOUD Act Sec. 103(c).

10 CLOUD Act Sec.104, 18 U.S.C. Sec. 2511(2)(j).

11 CLOUD Act Sec.105(a), 18 U.S.C. Sec. 2523(b).

12 As stated in footnote 5 above, while the U.S. government subjects non U.S.-based companies to data disclosure orders under the CLOUD Act because those companies may be subject to U.S. jurisdiction in some cases, it emphasizes that an executive agreement under the CLOUD Act does not expand U.S. jurisdiction (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*, pp.4-5 (Apr. 2019), *available at* https://www.justice.gov/opa/press-release/file/1153446/download).

13 There is a joint letter from several IT companies in which they expressed their opinion supporting the CLOUD Act bill (https://blogs.microsoft.com/wp-content/uploads/sites/149/2018/02/Tech-Companies-Letter-of-Support-for-Senate-CLOUD-Act-020618.pdf).

14 ACLU, *The Cloud Act Is a Dangerous Piece of Legislation* (Mar. 2018), *available at* https://www.aclu.org/blog/privacy-technology/internet-privacy/cloud-act-dangerous-piece-legislation; EFF, *The CLOUD Act: A Dangerous Expansion of Police Snooping on Cross-Border Data* (Feb. 2018), *available at* https://www.eff.org/ja/deeplinks/2018/02/cloud-act-dangerous-expansion-police-snooping-cross-border-data.

15 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* (Apr. 2019), *available at* https://www.justice.gov/opa/press-release/file/1153446/download.

which came into force on October 3, 2022, and also entered into an executive agreement with Australia on December 15, 2021. The U.S. also commenced negotiations for an executive agreement with Canada in March 2022, and has engaged in negotiations with the EU concerning an arrangement for collection of electronic evidence since September 2019.[16] At the time of entering into the executive agreement between the U.S. and the U.K., the U.S. government established a "CLOUD team"[17] within the Office of International Affairs (OIA) of the Criminal Division of the U.S. Department of Justice, which examines orders made pursuant to the agreement.[18]

2. Outline of the Proposed EU Electronic Evidence Regulation and Directive

(1) Background to Enactment

On April 17, 2018, the European Committee submitted a proposed electronic evidence regulation and a directive, with the aim of allowing the police and judicial authorities to easily and expeditiously obtain necessary electronic evidence, such as e-mails and documents stored in the cloud, in order to investigate, prosecute, and render a judgment of guilty against criminals and terrorists.[19] The proposed Electronic Evidence Regulation and Directive are being deliberated via ordinary legislative procedures, and on January 20, 2023, the proposed Electronic Evidence Regulation[20] and Directive,[21] which were amended based on an agreement between the European Council and the European Parliament, were published. Below, we provide an explanation of the proposed Electronic Evidence Regulation and Directive, as amended.

As network-based services have developed, there have been more cases in which electronic evidence related to a crime is stored outside the country in which the relevant investigation takes place, or is stored by a service provider located in a country other than the country in which the relevant

---

16 Actions based on the CLOUD Act are summarized on the website of the U.S. Department of Justice <https://www.justice.gov/criminal-oia/cloud-act-resources>. There are several countries that analyze the impact of entering into an executive agreement on domestic laws based on each country's background and legal system (*see*, for example, a report by the Swiss Federal Department of Justice and Police (September 17, 2021) <https://www.bj.admin.ch/bj/de/home/publiservice/publikationen/berichte-gutachten/2021-09-17.html>, and the Review of the Search and Surveillance Act 2012 by the Ministry of Justice of New Zealand (June 27, 2017) <https://www.lawcom.govt.nz/sites/default/files/projectAvailableFormats/NZLC-R141-Review-of-the-Search-and-Surveillance-Act-2012-final_0.pdf>14.158-14.159).

17 U.S. Department of Justice, *Landmark U.S.-UK Data Access Agreement Enters into Force* (3 Oct. 2022), *available at* https://www.justice.gov/opa/pr/landmark-us-uk-data-access-agreement-enters-force.

18 The Office of International Affairs of the Criminal Division of the U.S. Department of Justice is in charge of prior examinations and other matters relating to certain subpoenas to U.S. persons located abroad (U.S. Department of Justice "CRIMINAL RESOURCE MANUAL" 279).

19 European Commission, *Security Union: Commission facilitates access to electronic evidence* (Apr. 17, 2018), *available at* https://ec.europa.eu/commission/presscorner/detail/en/IP_18_3343.

20 Council of the European Union, *Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings - Analysis of the final compromise text* (Jan. 20, 2023), *available at* https://data.consilium.europa.eu/doc/document/ST-5448-2023-INIT/EN/pdf.

21 Council of the European Union, *Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings - Analysis of the final compromise text* (Jan. 20, 2023), *available at* https://data.consilium.europa.eu/doc/document/ST-5449-2023-INIT/EN/pdf.

investigation takes place. In fact, requests for judicial cooperation frequently are made to countries where many service providers are located, and the number of such requests has increased. As a result, it takes significant time to obtain electronic evidence via requests for judicial cooperation in other countries. Against this background, each member state often seeks the voluntary cooperation of service providers directly by utilizing various procedures within the country. This tendency could lead law enforcement authorities, judicial authorities, and service providers needing to respond to legal requests to face legal uncertainty and potential conflicts of law, which can be seen as a fragmentation of the legal framework for obtaining electronic evidence. Therefore, in connection with transboundary judicial cooperation for production and preservation of electronic evidence, there was a need to establish certain rules, in accordance with the characteristics of electronic evidence, including an obligation for service providers included in the applicable scope of the relevant systems to respond directly to requests issued by another member state's authorities.

As such, the proposed Electronic Evidence Regulation and Directive were submitted in order to supplement the existing EU laws and clarify the rules applicable to law enforcement authorities, judicial authorities, and service providers in the area of electronic evidence while ensuring full compliance with fundamental rights.[22]

(2) Overview of the Proposed Electronic Evidence Regulation and Directive

The proposed Electronic Evidence Regulation and Directive essentially have three significant points, as discussed below.

First, the proposed Electronic Evidence Regulation will apply to service providers that offer services within the EU.[23] The proposed Electronic Evidence Directive will impose an obligation on service providers that have no bases in the EU to establish a representative, by which means the effective exercise of executive jurisdiction will be ensured.

Specifically, the production orders and the preservation orders provided for in the proposed Electronic Evidence Regulation are decisions that will be issued by a judicial authority in a member state that is bound by the proposed Electronic Evidence Regulation and Directive, and that will be addressed to a designated establishment or representative of a service provider that offers services within the EU and is located in another member state that is bound by the proposed Electronic Evidence Regulation and Directive.[24] The requirement of "a service provider offering services in the [EU]" was as a limitation, so that only service providers that have a "substantial connection based on specific factual criteria to the Member State(s)"[25] will be subject to the regulation.

In addition, the proposed Electronic Evidence Directive requires that if a service provider that has legal personality and offers services within the EU is established in a member state that is bound by the proposed Electronic Evidence Regulation and Directive, the member state will cause the service provider to designate an establishment (entity) responsible for receiving, complying with, and enforcing decisions and orders. In addition, even if a service provider that has legal personality and

---

22 Preambles (7) through (9) of the proposed Electronic Evidence Regulation, Preambles (1) through (7) of the proposed Electronic Evidence Directive.

23 Article 3, Paragraph 1 of the proposed Electronic Evidence Regulation. The EU General Data Protection Regulation (EU/2016/679) (the "**GDPR**") and some of other EU laws use offering services within the EU as a factor for determining whether any connection exists (*see* Article 3, Paragraph 2(a) of the GDPR).

24 Article 2(1) and (2) of the proposed Electronic Evidence Regulation.

25 Article 2(4) of the proposed Electronic Evidence Regulation (*see* also Article 2(3) of the proposed Electronic Evidence Directive).

offers services within the EU is not established within the EU, a member state that is bound by the proposed Electronic Evidence Regulation and Directive will be required to cause service providers offering services within that state to designate a representative (legal or natural person) responsible for receiving, complying with, and enforcing decisions and orders.[26] The designated establishment or representative must reside in a member state in which the service provider offers services (a member state that is bound by the proposed Electronic Evidence Regulation and Directive) and must be subject to the execution procedures.[27] Thus, the proposed Electronic Evidence Directive will require a service provider offering services within the EU to designate an establishment or representative in a member state that is bound by the proposed Electronic Evidence Regulation and Directive, and in which the service provider offers services; therefore, the system ensures that a production order or a preservation order can be executed even if a service provider has no establishment within the EU.

Second, when comparing a preservation order and a production order, the latter involves a more significant infringement on rights. Therefore, while a preservation order covers all criminal offences and execution of a custodial sentence or a detention order of at least four months, a production order covers only the limited extent necessary and reasonable for certain criminal procedures, taking into account the rights of a suspect or defendant.[28] Furthermore, the handling differs depending on the type of data; if traffic data (excluding data requested for the sole purpose of identifying the user) or content data that is subject to a production order is protected by immunities and privileges granted under the law of the member state where the service provider is addressed, or is protected by rules on determination and limitation of criminal liability relating to freedom of press and freedom of expression in other media, the issuing authority[29] cannot issue a production order.[30]

"Electronic evidence" consists of subscriber data, traffic data, and content data[31]; the target subject to a production order differs depending on the type of data, as indicated below.

---

26 In addition, a member state that joins the proposed Electronic Evidence Regulation and Directive is required to cause service providers that are offering services within the country, are established in member states not bound by the proposed Electronic Evidence Regulation and Directive, and offer services within the EU, to designate a representative (legal or natural person) responsible for receiving, complying with, and enforcing decisions and orders.

27 Article 3, Paragraphs 1 and 2 of the proposed Electronic Evidence Directive.

28 Preambles (30) and (31) of the proposed Electronic Evidence Regulation.

29 While a production order for subscriber data and data requested for the sole purpose of identifying the user may be issued by a judge, a court, an investigating judge, a public prosecutor, or any other competent authority acting in its capacity as an investigating authority in criminal proceedings in a specific case and in accordance with national law, public prosecutors are excluded from the authorities that can issue a production order for traffic data (excluding data requested for the sole purpose of identifying the user) and content data (Article 4, Paragraphs 1 and 2 of the proposed Electronic Evidence Regulation). A public prosecutor may also issue a preservation order, regardless of the type of data (Article 4, Paragraph 3 of the proposed Electronic Evidence Regulation).

30 Article 5, Paragraph 7 of the proposed Electronic Evidence Regulation.

31 Article 2(6) of the proposed Electronic Evidence Regulation.

Type of Data	Content of Data	Target Subject to a Production Order
Data requested for the sole purpose of identifying the user	IP addresses and, where necessary, the relevant source ports and time stamps (date/time), or technical equivalents of these identifiers, and related information, where requested by law enforcement authorities for the sole purpose of identifying the user in a specific criminal investigation[32]	• All criminal offences • Execution of a custodial sentence or a detention order of at least four months[33]
Subscriber data	Any data held by a service provider relating to subscription to its services, pertaining to: (a) the identity of a subscriber or customer such as a provided name, date of birth, postal or geographic address, billing and payment data, telephone number, or email address, and (b) the type of service and its duration including technical data and data identifying related technical measures or interfaces used by or provided to the subscriber or customer at the moment of initial registration or activation, and data related to the validation of the use of service, excluding passwords or other authentication means used in lieu of a password that are provided by a user, or created at the request of a user[34]	
Traffic data (excluding data requested for the sole purpose of identifying the user)	(a) data related to the provision of a service offered by a service provider, which serves to provide context or additional information about the service and is generated or processed by an information system of the service provider, such as the source and destination of a message or another type of interaction, data on the location of the device, date, time, duration, size, route, format, the protocol used and the type of compression including electronic communications metadata, and (b) data relating to the commencement and termination of a user access session to a service such as the date and time of use, the log-in to and log-off from the service other than subscriber data[35]	• Criminal offences punishable in the issuing State by a custodial sentence of a maximum of at least three years • Offences related to cashless payments, offences related to sexual abuse of a child, and offences related to information systems, all or part of which were made through information systems • Terrorism and related offences • Execution of a custodial sentence or a detention order of at least four months, imposed for the aforementioned criminal offences[36]
Content data	Any data in a digital format, such as text, voice, videos, images and sound, other than subscriber or traffic data[37]	

32 Article 2(8) of the proposed Electronic Evidence Regulation.

33 Article 5, Paragraph 3 of the proposed Electronic Evidence Regulation.

34 Article 2(7) of the proposed Electronic Evidence Regulation.

35 Article 2(9) of the proposed Electronic Evidence Regulation.

36 Article 5, Paragraph 4 of the proposed Electronic Evidence Regulation.

37 Article 5, Paragraph 4 of the proposed Electronic Evidence Regulation.

The differences in the subjects to which these orders are applicable are based on the intention to establish stricter requirements for traffic data (excluding data requested for the sole purpose of identifying the user) and content data because their value as evidence is higher than that of subscriber data and data requested for the sole purpose of identifying the user, but they are highly sensitive data and the degree of infringement of rights created by these orders is significant. The threshold of criminal offences punishable by a custodial sentence of a maximum of at least three years was selected with the view of ensuring a balance between efficiency in criminal investigations and protection of rights, in accordance with the principle of proportionality (also based on a balance of penalties among the member states).[38] Since certain grounds for refusal of a production order are provided, production orders ensure protection of the rights of the addressees of production orders, service providers, and Data Subjects. Grounds for refusal include where there are substantial grounds to believe, on the basis of specific and objective evidence, that the execution of the production order would entail a manifest breach of a relevant fundamental right, as set out in Article 6 of the Treaty on European Union and the Charter of Fundamental Rights of the European Union, where the execution of the production order would be contrary to the principle of ne bis in idem, and other relevant situations.[39]

Third, the issuing authority is required to inform the Data Subject about the data production without undue delay[40]; thus, a mechanism to ensure transparency is embedded in the regulation.[41] If the issuing authority so informs the Data Subject, information about the applicability of each country's law for seeking remedies against the production order must be provided in a timely manner, and it is necessary to ensure that remedies can be exercised effectively.[42] However, an authority that issues a production order or a preservation order may delay, restrict, or omit informing the Data Subjects in order to avoid obstructing official or legal inquiries, investigations or procedures, to avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties, to protect the rights and freedoms of others, and for other relevant reasons.[43]

==========

Column (i): Discussions on Government Access in the OECD

As an international framework for the issues considered in this report, discussions on legal provisions related to government access to personal data held by private sector entities, called "government access," are progressing in international forums held by the OECD and other organizations.

---

38 Preamble (31) of the proposed Electronic Evidence Regulation.

39 Article 10a, Paragraph 1, Preamble (42)(a) through (f) of the proposed Electronic Evidence Regulation.

40 Article 11, Paragraph 1 of the proposed Electronic Evidence Regulation.

41 A similar mechanism can be seen in the EU Digital Services Act, which came into force on November 16, 2022. If a brokerage service provider receives an order from a judicial authority or an administrative authority to provide information regarding a recipient of the service, the service provider is required to provide information, including the reason for the order and the corrective actions, to the recipient, at the latest, by the time the order is performed (Article 10, Paragraph 5).

42 Article 11, Paragraphs 1 and 4; Article 17, Paragraph 3 of the proposed Electronic Evidence Regulation.

43 Article 11, Paragraph 2 of the proposed Electronic Evidence Regulation. Article 13, Paragraph 3 of the Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision (2008/977/JHA) *available at* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016L0680-20160504

These discussions are based on an awareness of the fact that while government access is considered necessary to ensure the security of citizens by preventing crimes and protecting national security, government access may infringe human rights, including the right to privacy, and may have an adverse impact on the global economy by impeding data distribution, if it conflicts with democratic values and the rule of law or is made in an unlimited, unreasonable, arbitrary, or disproportionate manner.[44]

On December 14, 2022, the Declaration on Government Access to Personal Data Held by Private Sector Entities (the "**OECD Government Access Declaration**"),[45] which contains seven principles for government access, was adopted at the ministerial meeting of the OECD's Committee on Digital Economy Policy.

This declaration defined the "government access" to which the declaration applies as access to and processing of personal data in the possession or control of private sector entities when governments are pursuing law enforcement and national security purposes within their respective territories, in accordance with their national legal frameworks, and clarified that this includes situations where countries have the authority under their national legal frameworks to mandate that private sector entities provide data to the government when the private sector entity or data are not located within their territories. Thus, the OECD Government Access Declaration specifies that cross-border acquisitions of data for investigative purposes, on which this report focuses, are within the scope of the declaration, and is worth focusing on.

The seven principles for government access set forth in the declaration, and an outline thereof, are as set forth below.

---

44 *See* the OECD Government Access Declaration mentioned below.

45 OECD, *OECD/LEGAL/0487*, (Dec. 14, 2022), *available at* https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0487#translations.

Seven Principles in the OECD Government Access Declaration
1. Legal basis Government access is provided for and regulated by the country's legal framework, which is binding on government authorities and is implemented by democratically established institutions operating under the rule of law. The legal framework sets out the purposes, conditions, limitations, and safeguards for government access, so that individuals have sufficient guarantees against the risks of misuse and abuse.
2. Legitimate aims Government access supports the pursuit of specified and legitimate aims. Government access is carried out in a manner that is not excessive in relation to the legitimate aims. Governments do not seek access to personal data for the purpose of suppressing criticism, or disadvantaging persons solely on the basis of characteristics including, but not limited to: ethnicity, gender identity or expression.
3. Approvals The legal framework establishes prior approval ("**approval**") requirements for government access, to ensure that access is performed in accordance with applicable standards, rules, and processes. The requirements are commensurate with the degree of interference with privacy and other human rights that will occur as a result of government access. Stricter approval requirements are in place for cases involving more serious interference.
4. Data handling Personal data acquired through government access can be processed only by authorized personnel. This processing is subject to requirements, which include putting in place measures to maintain privacy, security, confidentiality, and integrity. Internal controls are put in place to prevent data loss or unauthorized data access.
5. Transparency The general legal framework for government access is clear and easily accessible. Mechanisms exist for providing transparency about government access, and include public reporting by oversight bodies on government compliance with legal requirements and with procedures for requesting access to government records.
6. Oversight Mechanisms exist for effective and impartial oversight, to ensure that government access complies with the legal framework. Countries' oversight systems are comprised of bodies with powers that include the ability to obtain relevant information, conduct investigations, and address non-compliance.
7. Redress The legal framework provides individuals with effective judicial and non-judicial redress to identify and remedy violations of the national legal framework. These redress mechanisms take into account the need to preserve the confidentiality of national security and law enforcement activities. This may include limitations on the ability to inform individuals of whether their data was accessed or whether a violation occurred.

As stated above, the OECD Government Access Declaration sets forth comprehensive principles relating to government access. Taking into account the fact that the OECD member states, including the U.S., the EU member states, and Japan, will comply with this declaration, it can be viewed as providing the basis to consider specific domestic and international rules on government access, including government acquisition of personal data held by private sector entities domestically and overseas for investigative purposes in the future (for example, this declaration could be referenced when considering entering into executive agreements with foreign governments, as discussed in **VI** below).

Furthermore, countries that will comply with the OECD Government Access Declaration, including Japan, will be required to assess the consistency between the existing legal systems applicable to acquisition of the aforementioned data for investigative purposes (for example, rules contained in the Code of Criminal Procedure of Japan) and the declaration, and to promptly correct any inconsistencies or inadequacies.

==========

==========

Column (ii): Efforts of the Internet & Jurisdiction Policy Network (I&JPN)

The Internet & Jurisdiction Policy Network ("**I&JPN**") is a nonprofit organization incorporated in Paris, France in 2012. It has made efforts to enhance legal interoperability and to mitigate the tensions between national jurisdictions in cyberspace, in order to address the issues arising from the internet spreading beyond borders and national jurisdictions. Specifically, I&JPN launched programs addressing three issues: (i) data and jurisdiction, (ii) content and jurisdiction, and (iii) domain and jurisdiction; contact groups in the I&JPN consisting of multiple stakeholders are considering these issues and making various proposals.

In March 2021, the I&JPN released a series of "Toolkits," as the results of the efforts made through programs (i) through (iii) above, which include the protocols for establishing political frameworks and responses to these issues.[46] For example, the Toolkit on "Cross-border Access to Electronic Evidence,"[47] which is a product of the contact group for data and jurisdiction, presents the core components of systems that should be built for cross-border access to electronic evidence and the regime standards relating to these core components.

---

46 Internet & Jurisdiction Policy network, *News: Download the I&JPN Toolkits* (March 2021) *available at* https://www.internetjurisdiction.net/news/toolkits.

47 Internet & Jurisdiction Policy network, *Toolkit: Cross-Border Access to Electronic Evidence* (March 2021), *available at* https://www.internetjurisdiction.net/uploads/pdfs/Internet-Jurisdiction-Policy-Network-21-103-Toolkit-Cross-border-Access-to-Electronic-Evidence-2021.pdf.

IV. Issues Regarding Investigating Authorities' Obtainment and Use of Data Held by Companies Under Japanese Law

With the spread of the Internet, a large volume of data has come to be stored not only on terminals owned and used by individuals but also on servers managed[48] by companies. The SCA, as amended by the CLOUD Act, sets out procedures by which investigating authorities can access a large volume of data held by companies. On the other hand in Japan, while an amendment to the Code of Criminal Procedure in 2011 put in some sort of legal order investigative procedures for obtaining data stored on servers managed by companies, due to the subsequent spread of cloud services and for other reasons, the volume of data held by companies is dramatically increasing.[49] Hence, we will first analyze issues related to the laws and regulations of Japan concerning obtaining data held by companies for investigative purposes.

1. Investigative Method for Obtaining Data Held by Companies and Associated Issues

(1) Analysis of the Current Situation

The method by which an investigating authority can obtain data stored on a server managed by a company can be classified into roughly three categories (*see* **Figure**).

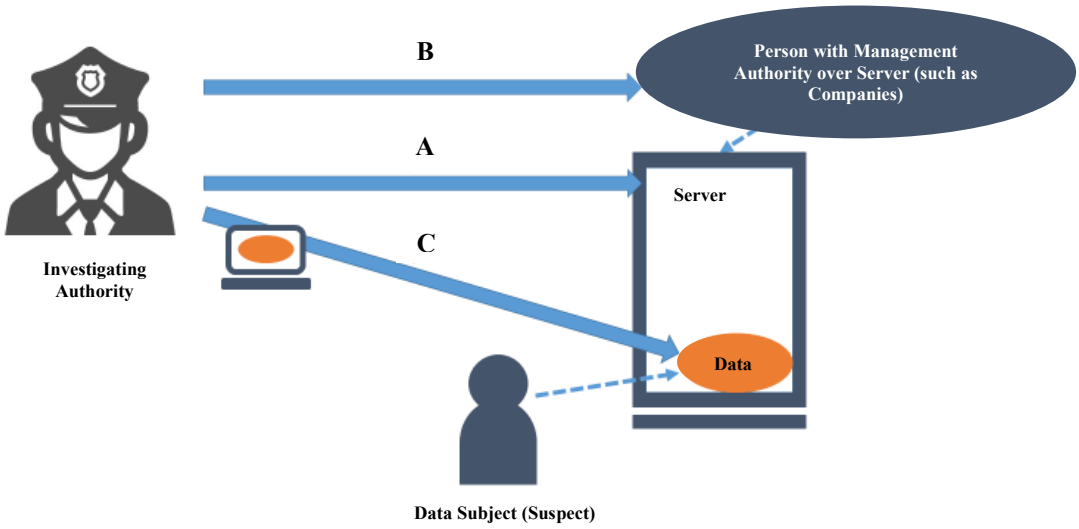

Figure: Classification of means by which an investigating authority obtains data stored on a server managed by a company

---

48 In this report, the term "manage" is used to mean, collectively, cases in which a company has the authority to manage a specific server based on its ownership or title to the server and cases in which a company has the authority to use a storage area in a specific server. A company or entity that has the authority to manage such a server may be referred to as a "person with management authority."

49 It is predicted that in 2025, 49% of the world's stored data will reside in public cloud environments (i.e., cloud environments provided by cloud service providers) (IDC, *The Digitization of the World - From Edge to Core*, p.4 (November 2018), *available at* https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf).

A. Seizing a Server on Which Data Is Stored

First, an investigating authority may seize the server on which the targeted data is stored (Article 218, paragraph (1) of the Code of Criminal Procedure). Alternatively, it is also possible for an investigating authority to copy only the targeted data stored on the relevant server onto another recording medium and then to seize the other recording medium (Article 222, paragraph (1); Article 110-2 of the same code).

In order to file a request for a warrant for these procedures, it is necessary to identify the relevant server as an article to be seized. However, in many cases, it is now difficult or impossible to identify the relevant server as an item to be seized because, in cloud services, data tends to be dispersed and stored on multiple unspecified servers, and companies often refuse to disclose the location of their servers. Moreover, even if the server on which the targeted data is stored can be identified, if the server is located overseas, a Japanese investigating authority's seizure of the server constitutes an exercise of jurisdiction in a foreign country, which constitutes an infringement of that country's sovereignty. Therefore, where servers are located outside of Japan, it is nearly impossible to seize the servers themselves (*see* **V.1.(2)** below).

B. Seeking Data Disclosure from a Person with Management Authority over the Server on Which Data Is Stored

Second, an investigating authority may request companies managing the server on which data is stored to disclose the targeted data.

If done by way of compulsory measure, the investigating authorities may compel a person with management authority over the relevant server to record the targeted data onto another recording medium and may then seize that other recording medium (Article 218, paragraph (1) and Article 99-2 of the Code of Criminal Procedure). In such a seizure warrant with an order to produce a copy of records, rather than an "article to be seized," the item specified to be produced is an "electromagnetic record to be recorded or printed out" (i.e., data to be disclosed)[50]; therefore, it is not necessary to identify the server on which the targeted data is stored. However, seizure via an order to produce a copy of records has the following disadvantages. First, in order to implement seizure via an order to produce a copy of records, the investigating authorities are required to actually go to the place where a person with management authority (i.e., the person subject to the relevant order) is located, present a warrant, have that person record the data in a recording medium, and then physically seize the recording medium. In addition, while seizure via an order to produce a copy of records is a compulsory measure based on a warrant, no method to enforce this measure has been legally established by which to ensure its effectiveness; thus, if a person with management authority, who is the person subject to the relevant disposition, does not cooperate voluntarily, the investigating authorities cannot obtain data sought.

Given these circumstances, in March 2022 the Study Group Regarding Use of Information and Communication Technology in Criminal Proceedings, established within the Ministry of Justice, publicly released a report; in this report, the Study Group proposed a system, pursuant to which investigating authorities can cause a person keeping relevant data to provide data online pursuant to a warrant issued by a judge, where necessary to investigate a crime (effectively excluding the "seizure" from "seizure via an order to produce a copy of records," and thereby limiting it to an "order to

---

50 The Training and Research Institute for Court Officials, *Warrant Practice (3rd ed.)*, p. 231 (Shiho Kyokai, 2017)

produce a copy of records")[51] Following this, the Criminal Law (pertinent to information and communications technologies) Subcommittee, which was established within the Legislative Council of the Ministry of Justice in July 2022, is considering the establishment of such a system (the "**Order to Provide Electromagnetic Records**").[52]

On the other hand, as a method that does not constitute a compulsory measure, an investigating authority may request that a person with management authority over the relevant server submit the targeted data using an official inquiry concerning matters related to an investigation without a warrant (Article 197, paragraph (2) of the same code).

C. Obtaining Data by Accessing the Server on Which Data is Stored

Third, an investigating authority may access the server on which the targeted data is stored through a client terminal, such as a terminal held by the relevant suspect, to obtain data (hereinafter, this investigative method is referred to generally as "**Remote Access**").

The Code of Criminal Procedure has provisions that explicitly authorize this method and specify the method of copying data from a recording medium (server) connected via telecommunication lines to a computer that is a client terminal to the computer or other recording medium, and then seizing the client terminal or other recording medium (Article 99, paragraph (2); Article 218, paragraph (2) of the same code; Remote Access pursuant to these provisions is referred to hereinafter as "**Remote Access Under the Code of Criminal Procedure**"). However, with regard to Remote Access Under the Code of Criminal Procedure, the Code only provides for a measure in which "those electromagnetic records may first be copied from the recording medium onto that computer or some other recording medium, and then that computer or other recording medium may be seized," so Remote Access is required to be implemented before the client terminal is seized. Thus, this procedure cannot be used in situations where access to the targeted data is possible only after the client terminal is seized (for example, where a password necessary to access the data is unknown at the time of conducting the seizure, or where a particular app is required to be launched).

Given these circumstances, the following approaches have been proposed. The first approach is that after seizing a client terminal, an investigating authority may be able to again request and acquire a seizure warrant that allows it to copy data through Remote Access Under the Code of Criminal Procedure in order to access the server. However, some question the necessity for conducting a seizure again given that the client terminal has already been seized and that an investigating authority is needing Remote Access, which is ancillary to the seizure.[53]

As a second approach, an investigating authority may access, recognize and copy the targeted data as part of an inspection of the server (Article 218, paragraph (1) of the same code). With respect to this investigative method, it may be necessary to consider whether such an approach is within the scope of an "inspection" of the server. Even if it is within such scope, Remote Access was reduced to statutory form in an amendment of the Code of Criminal Procedure in 2011; therefore, it has been

---

51 Study Group Regarding Use of Information and Communication Technology in Criminal Proceedings, *Summary Report by Study Group Regarding Use of Information and Communication Technology in Criminal Proceedings*, p. 13 (March 2022) (https://www.moj.go.jp/content/001368581.pdf).

52 *See* Criminal Law (pertinent to information and communications technologies) Subcommittee of the Legislative Council, Material 11 entitled *Basis for Consideration (Related to Matters for Ad visory (1)* distributed at the 7th meeting (https://www.moj.go.jp/content/001389630.pdf), Part 1-3, 1(2).

53 Hiroki Sasakura, *Cloud Investigation*, in Kuniji Shibahara et al., *Economic Criminal Law—Practice and Theory*, p. 575 (Shojihomu, 2017), Toshihiro Kawaide, *Issues on Criminal Procedure Law*, p. 113 (Tachibana Shobo, 2019)

pointed out that Remote Access by other means might not be permissible. However, several commentators support this investigative method.[54]

In addition, an investigating authority may conduct a voluntary investigation through Remote Access with effective, voluntary consent from a person who has authority to access the server where the relevant data is kept (*see* 2021 Supreme Court Decision).[55]

(2) Collaboration Between Investigating Authorities and Companies

As stated in **(1)** above, each of the methods of obtaining data held by companies for investigative purposes under the current laws has certain limitations. Regarding these issues, while it is necessary to consider legal reform, as analyzed in **(3)** below, from a mid- to long-term perspective, at the same time it is also necessary to consider a roadmap to address the present issues through cooperation and collaboration between investigating authorities and companies, as stated in **II** above.[56]

---

54 Yokohama District Court, Judgment, March 17, 2016, LEX/SB25542385; Tokyo High Court, Judgment, December 7, 2016, Kokeishu [*High Court Criminal Case Report*], vol. 69, no. 2, p. 5; Hiroki Sasakura, *Investigations in Cyberspace*, Hogaku Kyoshitsu, no. 446, pp. 31, 35-36 (2017); Toshihiro Kawaide, *Issues on Criminal Procedure Law* (Tachibana Shobo, 2019), pp. 114-115. *See* also Supreme Court, Judgment, March 15, 2017, Keishu [*Criminal Case Report*], vol. 52, no. 4, p. 275 (hereinafter referred to as "**2017 GPS Supreme Court Judgment**"), which rendered a decision on whether GPS investigation is permissible under an inspection warrant.

55 However, people now often possess an enormous amount of data, including a considerable amount of highly private information; therefore, the privacy of that data is comparable to privacy within a person's home. Thus, performing Remote Access with the voluntary consent of a person having authority to access data may be considered equivalent to performing a search of a person's home with the voluntary consent of the resident of the home. In light of the fact that Article 35 of the Constitution of Japan secures the right to not allow "entry" to a person's personal territory, which is equivalent to his/her "home" (*see* the 2017 GPS Supreme Court Judgment), and that Article 108 of the Code of Conduct for Criminal Investigation prohibits investigating authorities from performing a search of a home with the voluntary consent of the resident of the home, attention to privacy must be ensured with care, even when performing Remote Access via a voluntary investigation.

In addition, if investigating authorities attempt to perform Remote Access in a voluntary investigation while paying attention to the privacy of the person subject to the relevant disposition, it remains possible that the voluntariness of the consent will be rejected (*see*, among others, Osaka High Court, Judgment, September 11, 2018, Keishu [*Supreme Court Criminal Case Report*], vol. 75. no. 2, p. 220, which is the original judgment of the 2021 Supreme Court Decision); in light of the foregoing, it is possible that the stability of an investigation will not always be ensured automatically in the event of a voluntary investigation.

Considering these points, it is fair to state with regard to Remote Access that continuing consideration is required, to design more appropriate investigative methods other than voluntary investigations (*see* **V.1.(2)B** for matters to be considered where the relevant data is stored in a server outside Japan, or where this possibility cannot be ruled out).

56 In an Internet space, in particular, the person with management authority over the space is usually a private person, such as an Internet service provider, etc.; therefore, unlike roads or public facilities, over which a public institution has management authority, there is a higher necessity for an investigating authority to obtain information with the relevant company's cooperation when conducting an investigating activity on the Internet (*See* also, Tatsuhiko Yamamoto, *Sequel: Protection of Personal Information in the Internet Era—Centering on Effective Notice and Ambiguity of State*, in *Discussions on the Right to Privacy*, pp. 155, 168-169 (Shinzansha, 2017)).

A. Policies and Practices of Companies Responding to Orders and Requests from Investigating Authorities

According to the interviews conducted by the Study Group with domestic and foreign Internet and technology related companies, many domestic and foreign companies as a fundamental principle cooperate with a seizure via an order to produce a copy of records pursuant to a warrant issued after a court's judicial examination. In addition, it is understood that if a company is requested to make a report through an inquiry concerning matters related to an investigation as mentioned above, the company still has a legal obligation to make the report; in fact, companies seem to accept such inquiries in emergency cases, in particular.

In connection with companies' responses to these orders and requests from investigating authorities, some companies clearly specify in their terms of use or privacy policies that they will provide notice to users when they respond to orders or requests from investigating authorities. This may provide their users with an opportunity to lodge a complaint against the companies regarding their responses to orders or requests from investigating authorities. In addition, some companies release transparency reports in which they clarify the number of disclosure requests that they have received from investigating authorities and the number of cases in which they accepted these requests; thus, they have made efforts to enhance their transparency regarding their responses to investigating authorities (*see* **VII** below).

B. Further Use of Seizure via an Order to Produce a Copy of Records and an Order to Provide Electromagnetic Records

Given these companies' response policies and circumstances, it is desirable to see investigating authorities make further use of the means of seizure via an order to produce a copy of records to obtain data held by companies.

As stated in **(1)C** above, it is hard to say that Remote Access Under the Code of Criminal Procedure is convenient for investigating authorities. On the other hand, as stated in **A** above, many companies actually accept seizures via an order to produce a copy of records. In addition, there are cases where data that is subject to an investigation has been deleted from a client terminal but has not been deleted and is still stored on a server managed by a company.[57] Investigating authorities may be able to obtain the data through a person with management authority over the relevant server by performing a seizure via an order to produce a copy of records in such cases. In addition, as discussed in **V.1.(2)A** below, a seizure via an order to produce a copy of records is unlikely to be interpreted as an illegal exercise of enforcement jurisdiction, even if the targeted data is stored overseas, as long as the relevant seizure via an order to produce a copy of records is directed to a company subject to the jurisdiction of Japan. In this regard, a seizure via an order to produce a copy of records can be considered a more stable means of obtaining data stored on servers.[58]

Additionally, given the current heightened international awareness of privacy protection, it is anticipated that more companies will request a warrant instead of an inquiry concerning matters related to an investigation before disclosing data in the future. From this viewpoint, the means of

---

57 For example, where the user of a client terminal uses a cloud service, if data stored on the client terminal is deleted, there is a possibility that the data is stored on such cloud servers.

58 However, in recent years, domestic and foreign discussions have taken place regarding access to servers located outside Japan (*see* **V.1.(2)B.** below). It will be important for investigating authorities to choose an appropriate investigative method, based on the relevant situation, through which to request that a person with management authority over a server where relevant data is stored submit data (such as a seizure via an order to produce a copy of records held), or to obtain the data by accessing the server themselves (see **D.** below).

seizure via an order to produce a copy of records, which is a measure based on a warrant, should be utilized more extensively.[59][60]

Further, as discussed in **(1)B** above, the Legislative Council currently is considering the creation of an Order to Provide Electromagnetic Records so that investigating authorities can cause the person responsible for storage of relevant data to provide necessary data online, via a warrant issued by a judge. It is anticipated that this system also will be used in the future.

C. Collaboration Between Investigating Authorities and Companies in Connection with the Utilization of Seizure via an Order to Produce a Copy of Records and an Order to Provide Electromagnetic Records

As stated in **(1)B** above, in a warrant of seizure via an order to produce a copy of records, an "electromagnetic record to be recorded or printed out" is entered, rather than an "article to be seized."[61] If the "electromagnetic record to be recorded or printed out" is described in an overly general manner, it will cause difficulty for the companies to respond and also will be problematic in terms of protection of the Data Subject's rights. On the other hand, if overly specific identification is required, investigating authorities will not be able to request a warrant because, in many cases, they cannot specifically know in advance what type of data is stored, and in what form.[62]

Similar issues also may apply to situations involving an Order to Provide Electromagnetic Records, legislation for which is being considered currently.

Therefore, we expect investigating authorities and companies to seek ways to identify data that will be subject to seizure via an order to produce a copy of records or an Order to Provide Electromagnetic Records through cooperation and in a manner that will facilitate smooth collaboration.

Additionally, the specific protocol for presenting a warrant and submitting data can become an issue in the context of utilizing seizure via an order to produce copies of records or an Order to Provide Electromagnetic Records. The Legislative Council currently is considering digitization of requests for, and issuance and execution of, warrants (*see* also **(3)A** below). When considering these matters,

---

59 In the United States, the Supreme Court, focusing on invasion of privacy by the government's acquisition of location information held by wireless carriers in a continuing and comprehensive manner, decided that the government's acquisition of such data constituted a "search" under the Fourth Amendment to the United States Constitution and required a warrant (*Carpenter v. United States*, 138 S. Ct. 2206, 201 L. Ed. 2d 507, 2018). As an example of Japanese literature that introduces this decision, *see* Hiraku Tanaka, *Collection of Location Information in the "Bid Data Era" and the Fourth Amendment to the United States Constitution—Recent Case in the United States (Carpenter v. United States, 585 U.S. (2018))* in *Commemorative Collection for the 70th Anniversary of the Birth of Professor Masahito Inoue*, p.433 (Yuhikaku Publishing, 2019). Although it is necessary to wait for further discussions to determine what suggestions are viable for Japan, this decision can be referred to in the future as a decision made by focusing on an invasion of privacy regarding whether a warrant is required for an investigation to obtain data.

60 This direction also is consistent with the OECD Government Access Declaration (*see* **Column (i)** above), which provides, with regard to government access, that a system of prior approval and supervision should be developed.

61 In the United States, unlike in Japan, it is explicitly provided that information is also subject to search and seizure (18 U.S.C. §3111. (Property seizable by search warrant), Rule 41 (a)(2)(A) of the Federal Rules of Criminal Procedure). The scope of the search and seizure in the United States can accordingly be limited by identifying the scope of information to be searched for and seized.

62 Because of this issue, investigating authorities request a warrant after engaging in discussions with companies that own the data subject to the investigation.

it is important for investigating authorities to establish a protocol in collaboration with the companies that actually will submit data.

D. Points to Note Concerning Method by Which Investigating Authorities Obtain Data by Directly Accessing the Server Where the Relevant Data Is Stored

As stated in **(1)C** above, Remote Access Under the Code of Criminal Procedure can hardly be called convenient for investigating authorities. However, at least under the current Code of Criminal Procedure, Remote Access (including situations where performed as an inspection of servers or where performed as part of a voluntary investigation) cannot be ruled out, per se, as a useful method for investigating authorities because (among other reasons): (i) it enables investigating authorities to obtain data without going to the location of the relevant server or the person with management authority;[63] (ii) investigating authorities may obtain end-to-end encrypted data through users' client terminals, even if it cannot be decrypted by the business operator, including persons with management authority;[64] and (iii) investigating authorities may obtain data even where companies cannot be expected to submit the data voluntary.[65]

However, unlike investigative methods that require a person with management authority over the relevant server to submit data, such as seizure via an order to produce copies of records or an Order for Provision of Electromagnetic Records, Remote Access allows investigating authorities to obtain the target data without involving the companies that manage the server; thus, it raises issue of due process with regard to those companies. It is therefore advisable to introduce means of ensuring procedural fairness such as a notification mechanism, also with respect to companies (see **(3)B** below).

(3) Issues for Consideration Regarding the Design of Future Legal Systems

The following issues should be considered in the future with regard to methods for obtaining data held by companies.

A. Digitization of Warrant Proceedings and Online Data Submission

In order to maintain a proper balance between requests for judicial control through examination of warrants and requests for speedy investigations, it is important to consider digitization of warrant proceedings. In addition, in the interviews of domestic and foreign companies by the Study Group, a number of companies answered that it would be easier for them to cooperate with investigating authorities if online data submission is implemented.

---

63 If a system for an Order for Provision of Electromagnetic Records is established, investigating authorities will be able to request submission of data without going to the place where a person having management authority is located. Thus, we believe this advantage will be relatively small.

64 However, if the person subject to the relevant disposition is a suspect, and that person is forced to disclose passwords or to decode encrypted data, an issue may arise with regard to the privilege to refuse self-incrimination (Article 38, paragraph (1) of the Constitution of Japan) (*see* **3.(1)** below).

65 The Legislative Council currently is considering establishment of a policy to ensure the effectiveness of indirect enforcement of Orders to Provide Electromagnetic Records against persons subject to orders (Material 11 entitled, *Basis for Consideration (Related to Matters for Advisory (1),* distributed at the 7th meeting of the Criminal Law (pertinent to information and communications technologies) Subcommittee of the Legislative Council (https://www.moj.go.jp/content/001389630.pdf), Part 1-3, 2(4)). Accordingly, if a system for Orders to Provide Electromagnetic Records is established, this advantage may be relatively small.

In this respect, the Criminal Law (pertinent to information and communications technologies) Subcommittee of the Legislative Council is taking into consideration the proposals[66] made in the summary report by the Study Group Regarding Use of Information and Communication Technology in Criminal Proceedings and currently is considering digitization of warrant proceedings.[67] In addition, upon creation of a system for Orders for Provision of Electromagnetic Records, business operators located in distant places will be able to submit data online from their locations in response to warrants presented online.

How to ensure security in online presentation of warrants and online data submissions will be an issue.[68] In this respect, the Securities and Exchange Surveillance Commission will be a useful reference; it has built "Compliance WAN,"[69] a network connection using a dedicated line, as a system by which market players, including relevant authorities, can exchange information relating to unfair trade practices. In addition, some companies have built online systems of their own for communication with law enforcement authorities, and are ensuring security by building a closed environment instead of an open public environment, for example, by having investigating authorities register an e-mail address with an official domain.[70]

Further, if a legal system for Orders for Provision of Electromagnetic Records is created, and it becomes possible for authorities to present warrants online to business operators in a distant location and receive data submissions from them online, it also will be technically possible for them to dispatch an order to request that business operators located outside Japan submit data, which to date has been physically impossible. Whether international law permits investigating authorities to exercise their jurisdiction over a person with management authority over a relevant server, who is located in a foreign country, must be carefully considered (see **V.1.(2)A** below); however, we believe that the scope within which an exercise of jurisdiction is permitted may be extended in the future if the Second Additional Protocol to the Cybercrime Convention (see **V.2.(2)C** below), which provides for direct cooperation with a party located in another party, is ratified, or if a bilateral framework, such as executive agreements pursuant to the CLOUD Act, is built (see **VI.1.** below) in the future. We

---

66 Study Group Regarding Use of Information and Communication Technology in Criminal Proceedings, *Summary Report by Study Group Regarding Use of Information and Communication Technology in Criminal Proceedings*, pp. 9-12 (March 2022) (https://www.moj.go.jp/content/001368581.pdf).

67 *See* Criminal Law (pertinent to information and communications technologies) Subcommittee, Material 11 entitled, *Basis for Consideration (Related to Matters for Advisory (1),* distributed at the 7th meeting (https://www.moj.go.jp/content/001389630.pdf), Part 1-2.

68 *See* General Security Measures Meeting, *Further Promotion of Public-Private Collaboration in Cybercrime Investigations and Damage Prevention Measures*, p. 12 (April 2016) (https://www.npa.go.jp/bureau/cyber/pdf/h27_honpen.pdf), as discussions regarding online inquiry concerning matters related to an investigation.

69 Securities and Exchange Surveillance Commission, *Commencement of Use of "Compliance WAN"* (January 26, 2009) (https://www.fsa.go.jp/sesc/news/c_2009/2009/20090126.html).

70 One example in foreign countries is that, in the United States, an investigating authority generally seizes data through a secure portal site prepared by communications carriers. In addition, in France, the investigating authority requests and obtains data through an "International Judicial Interception Platform" (*See* Study Group Regarding Use of Information and Communication Technology in Criminal Proceedings, Material 33 for the 9th meeting, *Outline of the Legal System and Operation Concerning Use of Information and Communication Technology in Foreign Countries [Tentative and Updated Version]*(https://www.moj.go.jp/keiji1/keiji07_00022.html)). In addition, there is a platform (Post and Telecommunications Surveillance Service) (https://opendata.swiss/en/organization/dienst-ueberwachung-post-und-fernmeldeverkehr-uepf) in Switzerland for the exchange of data by law enforcement authorities and service providers, and law enforcement authorities in Switzerland use this service by paying fees to service providers.

therefore believe that it also will be necessary to consider legislation and the development of relevant systems necessary to dispatch an Order for Provision of Electromagnetic Records to business operators located outside Japan.[71]

B. Means to Ensure Procedural Fairness, Including a Mechanism for Notice

The Code of Criminal Procedure of Japan provides that the relevant type of warrant must be presented to a person who is subject to the relevant disposition, as a system to ensure fairness of investigative procedure using warrant (Article 222, paragraph (1); and Article 110 of the same code). However, when obtaining data held by companies for the purpose of investigating that data, at a minimum the interested parties include the Data Subject (such as suspects) and the person with management authority over the server (such as companies) (*see* Figure in **(1)** above); thus, fairness may not be sufficiently ensured only by simply ensuring procedural fairness in relation to the person who is subject to the relevant disposition. We therefore sort out matters that should be taken into consideration when ensuring procedural fairness in situations where the investigating authority requests that a person with management authority over the server where the data is stored submit data, and situations where the investigating authority directly accesses the server where the relevant data is stored, respectively.

(a) Where the Investigating Authorities Request that a Person with Management Authority Over a Server Where Data Is Stored Submit the Data

In situations where an investigating authority requests that a person with management authority over a server where relevant data is stored submit the data, a Data Subject who has a material interest in the data is not always subject to the relevant disposition. Therefore, it is necessary to consider not only the necessity of presenting a warrant to the person who is subject to the relevant disposition (such as the person with management authority over the relevant server), but also a method by which to ensure procedural fairness, that considers the interests of the Data Subject.

With regard to a request by an investigating authority to a person with management authority over a relevant server for submission of the relevant data, the person with management authority may play a role in responding appropriately to the request by taking into consideration not only the responding party's own interests but also the Data Subject's interests, by examining the effectiveness of the request in detail. However, if the Data Subject is not aware of the fact that a request for data submission has been made or of the fact that the data has been submitted in response to such a request, the Data Subject will lose the opportunity to state an objection or to receive relief for an infringement of rights or interests suffered by the Data Subject. Thus, from the perspective of protecting the rights and interests of the Data Subject, a legal system under which information will be provided to the Data Subject in a timely and appropriate manner should be considered important. For example, the proposed EU Electronic Evidence Regulation (see **III.2.(2)** above) legally requires that an issuing authority requesting the production or preservation of evidence notify the subject of the targeted data about the data submission without any unreasonable delay.[72] In addition, the Toolkit on "Cross-

---

71 In relation to this, whether an Order for Provision of Electromagnetic Records may be issued to a business operator located outside Japan through a representative or agent of the business operator established or designated in Japan pursuant to Japanese laws or regulations may also be an issue for discussion (*see* **V.1.(2)A** below).

72 Article 11, paragraph 1 of the proposed EU Electronic Evidence Regulation. The proposal also provides that when an issuing authority gives notice to a Data Subject, the issuing authority shall provide the Data Subject in a timely manner with information that the Data Subject may seek relief pursuant to the domestic laws of the member country, as stated below, and that this information shall ensure that the relief will be exercised effectively (the proposed EU Electronic Evidence Regulation, Article 17, paragraph 3).

Border Access to Electronic Evidence" released by I&JPN (*see* **Column (ii)** above) also provides, as a default rule, that a legal obligation to give notice to the Data Subject (user) must be imposed on a country that makes a request or dispatches an order for the submission of data.[73]

On the other hand, if notice of the submission of data is given to a Data Subject in the course of an investigation, and particularly when the Data Subject is a suspect or a party related to a suspect, the secrecy or effectiveness of the investigation may be impaired.[74] Considering this, the proposed EU Electronic Evidence Regulation provides, for example, that an issuing authority may delay, limit, or omit giving notice of data submission to the extent necessary and reasonable for purposes of avoiding interference with an investigation, ensuring national security, or other purposes.[75] The Toolkit on "Cross-Border Access to Electronic Evidence" by I&JPN states that if it is likely that an ongoing investigation will end in vain due to disclosure of information, the relevant issuing authority may delay giving notice to the Data Subject or keep the relevant request or order concerning data submission secret[76] for a certain period.[77] Further, under the OECD Government Access Declaration (*see* **Column (i)** above), while the importance of the interest in receiving information from individuals is suggested from the perspective of ensuring transparency and relief, it is also stated that this should be balanced with the need for maintaining confidentiality concerning national security and law enforcement activities.

Taking into consideration discussions in other countries or regions or international forums, we believe that it also is necessary to consider designing a legal system in Japan for the protection of the rights and interests of Data Subjects as a measure to ensure procedural fairness that considers the rights and interests of Data Subjects. This should be done by bearing in mind the timing and details of the

---

73 Internet & Jurisdiction Policy network, *Toolkit: Cross-Border Access to Electronic Evidence* (March 2021), *available at* https://www.internetjurisdiction.net/uploads/pdfs/Internet-Jurisdiction-Policy-Network-21-103-Toolkit-Cross-border-Access-to-Electronic-Evidence-2021.pdf, p.19.

74 One domestic precedent which addressed this problem is that, under the Guideline Regarding Pr otection of Personal Information in the Telecommunications Business, before the amendment in June 2015, when a telecommunications carrier was to provide GPS information from a user's mobile device in accordance with a request from an investigating authority, the carrier was requ ired to make the relevant user aware of the fact that their GPS information was being obtaine d, for example, by the sound of an alarm or vibration of the mobile device. However, as a res ult of the amendment in June 2015, this requirement was deleted because it impaired the effect iveness of investigations. For the purpose of this amendment, *see also*, the *(Proposed) Amend ment to the "Guideline Regarding Protection of Personal Information in the Telecommunications Business"* which is material relating to the procedures for public comment relating to the ame ndment to the commentary on the Guideline (2015) (https://search.e-gov.go.jp/servlet/PcmFileDow nload?seqNo=0000127697).

75 Article 11, paragraph 2 of the proposed EU Electronic Evidence Regulation; *Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA available at* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016L0680-20160504), Article 13, paragraph 3.

76 The Toolkit on *Cross-Border Access to Electronic Evidence* does not clearly state the method to preserve requests or orders for obtaining data; however, one conceivable method is to limit the details in the notice to the Data Subject and not clarify the purpose and background of obtaining the data.

77 Internet & Jurisdiction Policy network, *Toolkit: Cross-Border Access to Electronic Evidence* (March 2021), *available at* https://www.internetjurisdiction.net/uploads/pdfs/Internet-Jurisdiction-Policy-Network-21-103-Toolkit-Cross-border-Access-to-Electronic-Evidence-2021.pdf, p.19 (*see* **Column (ii)** above).

notice to be given to Data Subjects, as well as responses that should be required from persons having management authority over the relevant server who actually will receive an order for submission of data. On the other hand, when considering the form of such a system, it is necessary to specifically consider the way to balance the protection of the rights and interests of Data Subjects and the effectiveness of investigations, while referring to discussions in other countries or regions or in international forums, as discussed above.[78] When considering these issues, we believe that relevant systems existing under domestic laws also should be referenced, including the Act on Communication Interception for Criminal Investigation (the "**Communication Interception Act**"), which does not require an interception warrant to be presented to the communicating parties because the existence of the communication interception should not be known to the communicating parties in advance due to the nature of such disposition (*see* Article 10 of the same act). On the other hand, that act has a system for giving subsequent notice to the communicating parties (Article 30 of the same act).[79]

Further, we believe that in addition to a notice that gives an opportunity to object to the submission of data, it is important to consider the system by which such objections or relief can be made or provided. Persons having management authority over the relevant server, who actually will receive orders for submission of data,[80] as well as Data Subjects themselves, are expected to be covered by these systems. In this respect, the proposed EU Electronic Evidence Regulation and the Toolkit on "Cross-Border Access to Electronic Evidence" by I&JPN, referenced above, refer to the need for a system

---

78 For example, as a means to secure procedural fairness, there also is a system, in addition to giving notice, to have a third party attend the relevant investigation (Article 222, paragraph (1) and Article 114 of the Code of Criminal Procedure) (the 2017 GPS Supreme Court Judgment); thus, we believe that requiring the investigating authority to give notice in all cases of obtaining data owned by companies may not be the best solution.

79 Masahito Inoue, *Interception of Communications and Conversations as an Investigation Method*, pp. 81, 226 (Yuhikaku Publishing, 1997), Hidemi Suzuki, *What Are the Issues of the Communication Interception Act Under the Constitution?*, Hogaku Kyoshitsu, no. 232, p. 26, p. 26 (2000). A subsequent notice under the Communication Interception Act will be given to a party to the communications stated in an interception record, in situations where the interception record (Article 29 of the same Act) is prepared. This is because investigating authorities are permitted to intercept communications only to the minimum extent necessary to determine whether the communications constitute the communications to be intercepted as set forth in the warrant for interception (Article 14 of the same Act); however, it is not realistic to request that investigating authorities give notice in all situations involving the interception of communications for purposes of making those determinations, and this actually may cause an invasion of privacy in the course of giving notice.

80 Under the Code of Criminal Procedure, a person subject to seizure via an order to produce a copy of records by an investigating authority may file a quasi-appeal against the seizure (Article 430, paragraphs (1) and (2) of the Code of Criminal Procedure). The Legislative Council is currently discussing the inclusion of the provision of relevant data by Orders for Provision of Electromagnetic Records within the scope of the quasi-appeal (*see* Criminal Law (pertinent to information and communications technologies) Subcommittee of the Legislative Council, Material 11 entitled, *Basis for Consideration (Related to Matters for Advisory (1),* distributed at the 7th meeting (https://www.moj.go.jp/content/001389630.pdf), Part 1-3, 1(3)); it is anticipated that server-managing entities will file quasi-appeals not only after they submit data, but also before submitting data. In the United States, under the SCA, a service provider may file a motion with the court to modify or quash a relevant order, if the data for which disclosure is requested is unusually voluminous in nature or if compliance with the order otherwise would cause an undue burden on the provider (18 U.S. Code § 2703(d)). In addition, the CLOUD Act has established procedures for providers to file a motion to modify or quash the relevant order where the Data Subject is not a United States person and the relevant order would violate the laws of a foreign government with which the United States has an executive agreement (18 U.S. Code § 2703(h). See **III.1.(2)** above). As described, other countries have also established legal procedures for server-managing entities that have received an order to submit data to file an objection to the order before submitting the requested data.

whereby Data Subjects can make objections and receive relief, and also mention a policy that allows the use of existing legal systems or operations.[81]

(b) Where investigating authorities use the investigative method of directly accessing the server on which targeted data is stored

In cases where investigating authorities use the investigative method of directly accessing the server on which targeted data is stored, the problem of the company not becoming aware of access to the server under its management may arise, in addition to the problem of the attention to be paid to the interests of Data Subjects and due process as discussed in (a) above.[82]

In actual investigations in Japan, Remote Access is performed based on Article 218, paragraph (2) of the Code of Criminal Procedure (Remote Access Under the Code of Criminal Procedure), or as a inspection of the relevant server and pursuant to a voluntary investigation (*see* **1.(1)C** above); in any of these situations, no warrant is presented and no notice is given to persons having authority over the relevant server. On the other hand, the German Code of Criminal Procedure authorizes an investigating authority to access a server that is located in a place spatially away from the place subject to a search to preserve data in certain cases (Article 110, paragraph (3) of the German Code of Criminal Procedure); however, not only the person who is directly subject to the relevant disposition, but also the person with management authority over the relevant server must be notified of such disposition.[83]

Under the current Code of Criminal Procedure, Remote Access is performed as an investigation of "articles," such as a terminal to be seized or server. However, from a medium to long-term perspective, it may be worth considering the establishment of new proceedings for Remote Access, the purpose of which is obtaining data, per se (which is similar to the Order for Provision of Electromagnetic Records), and then designing a system that pays attention to due process with regard

---

81 The proposed EU Electronic Evidence Regulation provides that any persons whose data were sought via a European Production Order (for European Production Order, *see* **III.2.(2)** above) have the right to effective remedies against the production order (Article 17, paragraph 1). It also provides that the right must be exercised through a court pursuant to the domestic laws of the issuing state, and it does not limit the possible grounds upon which all persons can challenge the legality of the Order; these grounds include the necessity and proportionality of the Order (Article 17, paragraph 2). In addition, the proposal for the regulation provides that the terms and other conditions that apply to similar domestic cases shall apply to remedial procedures (Article 17, paragraph (4)). I&JPN's *Cross-Border Access to Electronic Evidence* Toolkit also states that a Data Subject must be ensured a meaningful opportunity to challenge the transmission and use of the Data Subject's data. It further states that the procedures for such challenges may be provided either through any applicable criminal proceeding in which government authorities seek to use these data, through data protection authorities, or through other available domestic statutory and civil remedies (Internet & Jurisdiction Policy Network, *Toolkit: Cross-Border Access to Electronic Evidence* (March 2021), *available at* https://www.internetjurisdiction.net/uploads/pdfs/Internet-Jurisdiction-Policy-Network-21-103-Toolkit-Cross-border-Access-to-Electronic-Evidence-2021.pdf, p.19.)

82 In case of performing Remote Access Under the Code of Criminal Procedure, a warrant containing the scope of servers subject to Remote Access must be presented to the holder of the relevant terminal (Article 219, paragraph (2) of the Code of Criminal Procedure). As the holder of the terminal and the Data Subject whose data is to be obtained via Remote Access are not always the same (although we believe that they often are the same), the problem of the Data Subject and due process may arise. In addition, when performing Remote Access as part of an inspection of servers, investigating authorities may perform Remote Access without seizing the terminal; accordingly, it is possible for investigating authorities to perform Remote Access without presenting a warrant to the Data Subject, and thus similar problems may arise depending on operational practices.

83 Kimihiro Ikeda, *Cybercrime Investigations in Germany*, Keijiho Journal, no. 51, pp. 42 and 44 (2017)

to persons having management authority over the relevant server, by referring to the German legal system described above.

C. Improving System to Impose an Obligation of Confidentiality on Companies

In connection with the discussion in **B** above, we believe that when investigating authorities issue a request or an order for the submission of data to a person with management authority over the relevant server,[84] it is necessary to consider imposing an obligation of confidentiality concerning the request or order on the person with management authority over the relevant server, with the view of ensuring the secrecy and effectiveness of investigative procedures.

Considering this, the Code of Criminal Procedure already has a system that imposes an obligation of confidentiality concerning requests for preservation of transmission history (Article 197, paragraph (5) of the same code). However, this system can be used only when the request concerns preservation of transmission history, and the existence of the disposition itself, such as seizure via an order to produce a copy of records, is not covered by the confidentiality obligation.[85] In addition, the confidentiality obligation may be imposed only on telecommunications service providers. Thus, this system of confidentiality for investigations is limited in usefulness for investigating authorities. From a mid- to long-term perspective, Japan should consider improving the system to impose a confidentiality obligation on companies.

On the other hand, in connection with this issue, the proposed EU electronic evidence regulation provides that service providers shall take necessary, state-of-the-art operational and technical measures to ensure the confidentiality, secrecy, and integrity of European Production Order Certificates (EPOC) and European Preservation Order Certificates (EPOC-PR)[86] and of the data produced or preserved.[87] It is worth referring to the U.S. SCA (*see* **III.1.(1)** above), which authorizes U.S. investigating authorities to seek an order suspending providers' notice to Data Subjects in certain cases.[88]

D. Legal Provisions on Use and Storage of Data Obtained by Investigating Authorities

As the investigative methods for obtaining data are utilized more often, a larger volume of data will be accumulated by investigating authorities. Therefore, ideal approaches to legal provisions for the use and storage of such data by investigating authorities should be considered.

---

84 The "person with management authority over the relevant server" does not include the relevant Data Subject unless the person with management authority over the relevant server is identical to the Data Subject.

85 Noriaki Sugiyama & Masayuki Yoshida, *Act for the Partial Amendment of the Penal Code to Respond to the Advancement of Information Processing (Second Half)*, Hoso-jiho, vol. 64, no. 5, pp. 55 and 117 (2012)

86 A European Preservation Order (Article 2(2) of the proposed Electronic Evidence Regulation), which orders the preservation of electronic evidence, is transmitted through an EPOC-PR, and a European Production Order (Article 2(1) of the proposed Electronic Evidence Regulation), which orders the submission of electronic evidence, is transmitted through an EPOC (Article 8, Paragraph 1 of the proposed Electronic Evidence Regulation).

87 Article 11, Paragraph 3 of the proposed Electronic Evidence Regulation.

88 18 U.S. Code § 2705(b). There is also an example of legislation that authorizes the U.S. investigating authorities to conduct an investigation without informing the person subject to the relevant disposition of the fact of the investigation's existence (PATRIOT Act, Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline over Monitoring Act of 2015(USA FREEDOM Act of 2015)).

For example, the European Court of Human Rights decided that the Police and Criminal Evidence Act 1984 of the United Kingdom violated Article 8 of the European Convention on Human Rights because the act allowed fingerprints and similar information collected from a suspect who was arrested on suspicion of a certain crime to be stored on a semi-permanent basis, regardless of whether the suspect subsequently was found guilty.[89] Following this decision, legal reform was effected by the Crime and Security Act 2010 in the United Kingdom, to specify the period for storage of fingerprints and similar information of a suspect who was not found guilty. In addition, the OECD Government Access Declaration (*see* **Column (i)** above) suggests that it is necessary to establish a legal framework that provides that personal data obtained through government access shall be handled pursuant to legal requirements, including measures to maintain privacy, security, confidentiality, and integrity, and shall be retained only for a legally permitted period, and that it is necessary to construct internal control systems to detect and prevent unauthorized use or modification of data.[90]

In Japan, the use and storage of data held by investigating authorities is governed not only by the Act on the Protection of Personal Information (formerly, the Act on the Protection of Personal Information Held by Administrative Authorities) to a certain extent,[91] but also by the regulations of the National Public Safety Commission, such as the Regulation Concerning Management and Handling of Suspect Photographs, the Regulation for Handling Fingerprints, and the DNA Handling and Recording Regulation, which set out matters concerning management and handling of information such as suspects' photographs, fingerprints, and DNA records, and state that these pieces of information must be deleted or destroyed where it is "no longer necessary… to store" them.[92] Data is used and stored by investigating authorities within the restrictions in these laws and regulations.[93] However, the court precedents are not clear as to which situations qualify as "no longer necessary… to store" data pursuant to these Regulations; therefore, it has been pointed out that there may be almost no cases where DNA data should be deleted pursuant to the regulations, depending on how these regulations operate.[94]

In addition, it also is necessary to consider what remedies should be provided to the Data Subjects whose data is illegally or inappropriately used or stored by investigating authorities. In this regard, while the Act on the Protection of Personal Information establishes the data subject's right to request disclosure of personal information held by administrative authorities (Article 76, paragraph (1) of the same Act), right to request corrections (Article 90, paragraph (1) of the same Act), and right to request suspension of use (Article 98, paragraph (1) of the same Act), the rights to make these requests do not apply to trials and dispositions by prosecutors in criminal cases (Article 124, paragraph (1) of the same Act), or to personal information recorded in documents relating to trials and seized articles (Article 53-2, paragraph (2) of the Code of Criminal Procedure). However, the judgment of the Nagoya District

---

89 S. and Marper v. The United Kingdom, 2008-V Eur. Ct. H.R. 167., available at https://www.echr.coe.int/Documents/Reports_Recueil_2008-V.pdf; Seishi Suei, *Issues on DNA-type Data Base*], Research & Legislative Reference Bureau, National Diet Library, Reference March 2011 issue, pp. 5, 6-12 (2011).

90 OECD, *OECD/LEGAL/0487*, (Dec. 14, 2022), Principle IV. (Data handling).

91 *See* Chapter V of the Act on the Protection of Personal Information.

92 Article 5 of the Regulation Concerning Management and Handling of Suspect Photographs, Article 5, paragraph (3) of the Regulation for Handling Fingerprints, and Article 7 of the DNA Handling and Recording Regulation.

93 *See* Order Dated February 17, 2023 of the Nagoya District Court, LEX/DB25594817.

94 *See* III.5.(3)B. of page 62 of Hanreijiho no. 2522 on the Order Dated January 18, 2022 of the Nagoya District Court. However, it is possible that some will indicate the difficulty to provide a uniform rule on "no longer necessary… to store."

Court dated January 18, 2022[95] upheld a request for deleting fingerprint, DNA, and facial photo data in a case where the plaintiff, for whom the judgment of not guilty had become final and binding, filed a petition for elimination of an infringement of moral rights, in which the plaintiff requested that their fingerprint, DNA, and facial photo data obtained by investigating authorities and data about the mobile phone owned by the plaintiff, be deleted. Looking at recent international discussions, the OECD Government Access Declaration suggests that remedies be granted for inappropriate access to or retention of personal data include deletion of the data and suspension of illegal processing of data.[96]

Based on the domestic trend and the international discussions mentioned above, discussions are expected to progress further on provisions regarding the use and storage of any data obtained by investigating authorities, and on remedies for Data Subjects in the event of illegal or inappropriate use and storage of data.[97] We believe it also is useful to understand the legal provisions that apply when data is obtained for investigative purposes and the legal provisions applicable to the use and storage of data after being obtained as a series and, on that basis, to consider the balance between both sets of legal provisions.[98]

E. Relationships with Other Laws and Regulations Aimed at Protection of Data

In creating an environment where investigating authorities are allowed to obtain data held by companies for investigative purposes under the Code of Criminal Procedure, it is also necessary to analyze how other relevant laws or regulations (*e.g.*, the following laws) may apply, in order to make sure that a company disclosing data to an investigating authority will not violate such laws or regulations.

(a) Telecommunications Business Act

The Telecommunications Business Act protects the secrecy of communications handled by telecommunications carriers (Article 4 of the Telecommunications Business Act). The scope of information protected under the secrecy of communications is broadly construed, and it is understood that all information by which the content of communications could be inferred are protected under the obligation to maintain secrecy of communications, including not only so-called content data (*e.g.*, the subject and main text of an e-mail, an attached file, content of the browsed website, voices during a call), but also so-called metadata (*e.g.*, transmission date and time, sender or recipient information, IP address, information on end users' terminal equipment).

---

95 As a commentary, Bujiro Kunita, Go Koyama, *Criminal Defense Report, Order Dated January 18, 2022 of the Nagoya District Court, Case No. 2018 (wa) 3020, LEX/DB25591643, Case seeking state redress, Order of deletion of fingerprint, facial photo, and DNA data of a man for whom a judgment of non-guilty became final and binding*, Quarterly Keiji Bengo, no. 113, pp. 100-104, etc.

96 OECD, *OECD/LEGAL/0487*, (Dec. 14, 2022), Principle VII. (Redress).

97 *See* also Member Ikeda's and Member Kubo's remarks in the minutes of the 7th meeting of the Criminal Law (pertinent to information and communications technologies) Subcommittee of the Legislative Council (https://www.moj.go.jp/content/001394233.pdf), pp. 27-29. It is important to consider those provisions with a view toward establishing national security systems for the use and storage of data (*see* George Shishido et al., *Present and Future of Information Legislation*, Ronkyu Jurist, vol. 20, p. 179 (2017)).

98 Daisuke Midori, *Legal Disciplines at the Time of Obtaining Information in Surveillance-type Investigations*, Horitsu-jiho, vol. 87, no. 5, pp. 65, 69 (2015), Tatsuhiko Yamamoto, *Meaning of Obtaining Information in Surveillance Investigations* in *Considering Right to Privacy*, pp. 67, 76-84 (Shinzansha, 2017), Tatsuhiko Yamamoto, *Meaning of Obtaining Information in Surveillance Investigations* in *Considering Right to Privacy*, pp. 89, 93-98 (Shinzansha, 2017)

In principle, telecommunications carriers holding personal data, including information protected under the obligation to maintain the secrecy of communications, are prohibited from providing such data to third parties, including governmental bodies. On the other hand, in exceptional cases where an act is performed in accordance with laws and regulations (Article 35 of the Penal Code; an "**Act Performed in Accordance with Laws and Regulations**"), including the cases where a seizure via an order to produce a copy of records is conducted, or cases where any other legal justification is found,[99] a telecommunications carrier's provision of such data to a third party will not be deemed to violate the act (*see* Article 4, paragraph (1) of the Telecommunications Business Act, Article 17, paragraph (8) of the Personal Information Protection Guidelines for Telecommunications Businesses,[100] and 3-7-3 of the Commentary on these Guidelines).[101]

However, given that telecommunications carriers are obliged to protect the secrecy of communications, it is understood that it is "inappropriate in principle" for them to provide information concerning investigation-related matters protected under the secrecy of communications in response to an inquiry concerning matters related to an investigation.[102]

Currently, discussions have taken place concerning the establishment of new investigative procedures involving Orders for Provision of Electromagnetic Records. From a mid- to long-term perspective, we believe that it is advisable to take measures which ensure that companies' provision of a certain specified scope of information to law enforcement authority would be categorically justified under the Telecommunications Business Act. Specifically, the investigation procedures to obtain data held by companies should be set forth explicitly and as types in laws and regulations that would cause such disclosures to be considered justified as "Acts Performed in Accordance with Laws and Regulations" under the criminal laws of Japan. This approach is more suitable than an approach invoking "acts performed in the pursuit of lawful business" (Article 35 of the Penal Code) or other legal justifications as justifications, both of which are examined on a case-by-case basis and thus less predictable and transparent. In legislating such laws and regulations, we believe that it is beneficial for government authorities to discuss with companies how to identify the relevant information.

It would be potentially useful to subdivide and refine the procedures for obtaining data by type or nature of data, such as metadata and content data, using legislation in other jurisdictions, such as the

---

99 George Shishido, *Memorandum on Secrecy of Communication* in *Commemorative Collection for the 70th Anniversary of the Birth of Professor Kazuyuki Takahashi, Aspects of Modern Constitutionalism (Second Half)*, pp. 487, 514 (Yuhikaku Publishing, 2013)

100 Personal Information Protection Committee, Ministry of Internal Affairs and Communications, *Personal Information Protection Guidelines for Telecommunications Businesses (Public Notice of the Personal Information Protection Committee and the Ministry of Internal Affairs and Communications No. 4 of March 31, 2022)* (March 2022) (https://www.soumu.go.jp/main_content/000805614.pdf)

101 Personal Information Protection Committee, Ministry of Internal Affairs and Communications, *Commentary on the Personal Information Protection Guidelines for Telecommunications Businesses (Public Notice of the Personal Information Protection Committee and the Ministry of Internal Affairs and Communications No. 4 of March 31, 2022)* (March 2022) https://www.soumu.go.jp/main_content/000805807.pdf)

102 Personal Information Protection Committee, Ministry of Internal Affairs and Communications, *Commentary on the Personal Information Protection Guidelines for Telecommunications Businesses (Public Notice of the Personal Information Protection Committee and the Ministry of Internal Affairs and Communications No. 4 of March 31, 2022)*, 3-7-1(1) (March 2022) https://www.soumu.go.jp/main_content/000805614.pdf). There is a view that in the case of an inquiry concerning matters related to an investigation, a bar to a finding of illegality is not necessarily found (Tatsuhiko Yamamoto, *Sequel: Protection of Personal Information in the Internet Era—Centering on Effective Notice and Ambiguity of State* in *Discussions on the Right to Privacy*, pp. 155, 178 (Shinzansha, 2017)).

EU and the United States, as a reference. However, when considering this potential option, it is necessary to ensure that these investigative procedures will be appropriate procedures for disclosing secret communications to third parties in compliance with due process of law, taking into account the existing scope of protection under the obligation to maintain the secrecy of communications, the obligation of telecommunications carriers to protect the secrecy of communications, and the protection of communicating parties' rights to and interests in the secrecy of communications. The amended Telecommunications Business Act that will come into force on June 16, 2023 (the "**Amended Telecommunications Business Act**," and the Enforcement Regulation of the Telecommunications Business Act that was amended pursuant to the Amended Telecommunications Business Act, the "**Amended Enforcement Regulation of the Telecommunications Business Act**")[103] designates telecommunications carriers that provide "telecommunications services that have a large impact on the interests of users"[104] ("**Designated Telecommunications Carriers**")[105] and provides for appropriate handling of "specified user information"[106] by Designated Telecommunications Carriers. We believe it is necessary to consider these new provisions in discussions on the process by which investigating authorities obtain data.[107]

(b) Act on the Protection of Personal Information

Under the Act on the Protection of Personal Information, personal information-handling business operators are, in principle, prohibited from providing a Data Subject's personal data to third parties (located in foreign countries) without obtaining consent from the Data Subject (Article 27, paragraph (1), Article 28 of the same act). As an example of one category of exceptions in which provision of personal data to third parties is deemed to be lawful, the act provides for "cases based on laws and regulations" (item (i) of the same paragraph). It is understood that where a company provides data held by it in response to an investigatory request for data, this is justified as falling within the category of "cases based on laws and regulations." In fact, in current investigative activities, where a company provides personal information to governmental bodies in accordance with an obligation imposed by a compulsory measure based on a warrant or an inquiry concerning matters related to an

---

103 Act Partially Amending the Telecommunications Business Act (Act No. 70 of 2022) (https://www.sangiin.go.jp/japanese/joho1/kousei/gian/208/pdf/s0802080482080.pdf).

104 *See* Article 22-2-20 of the Amended Enforcement Regulation of the Telecommunications Business Act (https://public-comment.e-gov.go.jp/servlet/PcmFileDownload?seqNo=0000246511). In summary, in the case of free telecommunications services, telecommunications services that have ten million or more users fall within the definition of "telecommunications services that have a large impact on the interests of users," and in the case of paid telecommunications services, telecommunications services that have five million or more users fall within that definition.

105 *See* Article 27-5 of the Amended Telecommunications Business Act.

106 In addition to information that touches upon the "secrecy of communications," information that can identify users and is part of the collective body (*e.g.*, database) of information that is systematically organized to allow a search of information that can identify a specific user using a computer falls within the definition of "specified user information" (Article 27-5 of the Amended Telecommunications Business Act, Article 22-2-21 of the Amended Enforcement Regulation of the Telecommunications Business Act).
The term "users," as used in the Amended Telecommunications Business Act, includes persons that are granted identification codes to use telecommunication services on an ongoing basis (*see* Article 2, item (vii)(a) of the same act, Article 2-2 of the Amended Enforcement Regulation of the Telecommunications Business Act), in addition to telecommunications carriers or persons that enter into an agreement to receive telecommunications services with persons that operate telecommunications businesses listed in Article 164, paragraph (1), item (iii) of the same act.

107 For the relationship between legal provisions concerning specified user information set forth in the Amended Telecommunications Business Act and executive agreements, *see* **VI.2.(2)A.** below.

investigation, this is also understood as falling within the category of "cases based on laws and regulations."[108]

Currently, discussions have taken place concerning the establishment of Orders to Provide Electromagnetic Records as a new investigative procedure by which to obtain data held by companies. From a viewpoint of ensuring predictability for interested parties, it is advisable to specify the procedures and conditions for a particular case to be deemed as falling within the category of "cases based on laws and regulations" under the Act on the Protection of Personal Information, as with the existing investigation procedures, in order to ensure that a company will not be deemed to violate the Act on the Protection of Personal Information provided that the company follows the statutory procedures.

Furthermore, it would be an option to subdivide and refine the procedures for investigating authorities to obtain data in accordance with the type or nature of personal data, or the risk level of invasion of privacy that may be caused by providing certain data, which could be organized into categories (based on the mechanism for involvement of Data Subjects or examinations by judicial bodies before or after the provision of data). In this respect, for example, the Personal Information Protection Guidelines for Telecommunications Businesses provide that when a telecommunications carrier is asked to obtain location information at the request of an investigating authority, it may obtain the location information only pursuant to a warrant issued by a judge.[109] In addition, the guidelines also provide that if a warrant is issued, a telecommunications carrier may provide the obtained location information to

---

108 For the view that in the case of receiving an inquiry concerning matters related to an investigation, the recipient of the inquiry is required to make a report and the recipient's provision of personal data is justified as being "based on laws and regulations" under the Act on the Protection of Personal Information, *see* Personal Information Protection Committee, *Guidelines Concerning the Act on the Protection of Personal Information (General Rules)*, 3-1-5 (September 2022; latest revision) (https://www.ppc.go.jp/files/pdf/230401_guidelines01.pdf), and Katsuya Uga, *New Commentary on the Act on the Protection of Personal Information*, p. 250 (Yuhikaku Publishing, 2021). The "Guidelines for Responses to Inquiries Concerning Matters Related to an Investigation" released by Japan Institute of Law and Information Systems (JILIS) in April 2020 (ver. 1 prepared on April 1, 2020) (https://www.jilis.org/proposal/data/sousa_guideline/sousa_guideline_v1.pdf) sets forth the following concept: since "'cases based on laws and regulations' are considered to mean situations where personal information is provided to a necessary and reasonable extent pursuant to laws and regulations in response to an inquiry concerning matters related to an investigation that was lawfully made," "for example, reporting information that is not related to investigations to an investigating authority in response to an inquiry concerning matters related to an investigation is not included in 'cases based on laws and regulations' and it is necessary to obtain consent from the Data Subject.

109 Personal Information Protection Committee, Ministry of Internal Affairs and Communications, *Personal Information Protection Guidelines for Telecommunications Businesses (Public Notice of the Personal Information Protection Committee and the Ministry of Internal Affairs and Communications No. 4 of March 31, 2022)*, Article 41, paragraph (4), (March 2022) (https://www.soumu.go.jp/main_content/000805614.pdf), and Personal Information Protection Committee, Ministry of Internal Affairs and Communications, *Commentary on the Personal Information Protection Guidelines for Telecommunications Businesses (Public Notice of the Personal Information Protection Committee and the Ministry of Internal Affairs and Communications No. 4 of March 31, 2022)*, 5-4-1 and 5-4-4 (March 2022) (https://www.soumu.go.jp/main_content/000805807.pdf).

others (investigating authorities) by obtaining the prior consent of users.[110][111] In connection with this, it also references the fact that the proposal of the E-evidence Regulation in the EU sets forth a difference in the subjects for which orders for submission can be used depending on the type of data (*see* **III.2.(2)** above).

2. Use of Data Obtained by Investigating Authorities in Criminal Trials

Even where investigating authorities obtain necessary data, issues still exist regarding the use of such data for trials.

(1) Methods of Examination of Data

The Criminal Law (pertinent to information and communications technologies) Subcommittee of the Legislative Council is considering the methods of examination of evidentiary documents prepared and managed by electronic means in open court, which will vary depending on the type and nature of information recorded in the data,[112] based on the proposals in the summary report by the Study Group Regarding Use of Information and Communication Technology in Criminal Proceedings.[113] Specifically, the following mechanisms are being considered: "read orally" when linguistic information is evidence; "display" when visual information is evidence; and "play" when auditory information is evidence.[114]

In this respect, it is necessary to note that when non-linguistic information is "displayed" or "played," the performance of hardware (screens, playback equipment, etc.) and software (images, videos, or other software to be played) used for that purpose may have a significant impact on judges' impressions. This issue is not necessarily specific to situations where data is submitted as evidence, but has existed where DVDs on which videos are recorded or tapes on which voices are recorded are submitted as evidence. However, if use of data obtained by investigating authorities in criminal trials becomes more common, it is possible that this issue may occur frequently. Further discussions are expected.

---

110 Personal Information Protection Committee, Ministry of Internal Affairs and Communications, *Personal Information Protection Guidelines for Telecommunications Businesses (Public Notice of the Personal Information Protection Committee and the Ministry of Internal Affairs and Communications No. 4 of March 31, 2022)*, Article 41, paragraph (2), (March 2022) (https://www.soumu.go.jp/main_content/000805614.pdf), and Personal Information Protection Committee, Ministry of Internal Affairs and Communications, *Commentary on the Personal Information Protection Guidelines for Telecommunications Businesses (Public Notice of the Personal Information Protection Committee and the Ministry of Internal Affairs and Communications No. 4 of March 31, 2022)*, 5-4-2 (March 2022) (https://www.soumu.go.jp/main_content/000805807.pdf).

111 The Commentary on the Personal Information Protection Guidelines for Telecommunications Businesses states that it is "strongly recommended" that acquisition or use of even location information that does not constitute the "secrecy of communications" under the Telecommunications Business Act should be limited to situations where consent is obtained from the user or there is a bar to the finding of illegality (*see* 5-4-1 and 5-4-2).

112 In addition to this, it is being considered whether metadata, such as property information, is subject to examination.

113 Study Group Regarding Use of Information and Communication Technology in Criminal Proceedings, *Summary Report of the Study Group Regarding Use of Information and Communication Technology in Criminal Proceedings*, pp. 18-19 (March 2022) (https://www.moj.go.jp/content/001368581.pdf).

114 *See* distributed material 11 for the 7th meeting of the Criminal Law (pertinent to information and communications technologies) Subcommittee of the Legislative Council, *Working Draft for Discussions Related to Advisory Matter "1,"* 1-5 1 (https://www.moj.go.jp/content/001389630.pdf).

(2) Methods to Ensure the Authenticity and Accuracy of Data

It is necessary to consider the means by which courts will ensure that the processes of collecting, selecting, and processing data submitted for trial were not arbitrary and that the acquisition method and acquiring party ensured the authenticity and accuracy of the data, in a situation where the authenticity and accuracy of the data are in doubt.[115] The Rules on Analysis of Information Technology in its Article 2, paragraph (1) provides that "Measures must be taken so that the subject of the analysis of information technology will maintain its probative value in a trial."

Specifically, we believe that if the authenticity and accuracy of data to be submitted as evidence are in doubt, investigating authorities could include the process of analyzing of the data in evidence together with the data, and submit an analysis report for trials. We assume that such an analysis report results would contain the place where the analysis was conducted, the model number and product number of the subject recording medium, the hash values[116] of the recording medium or each file, etc., the analysis protocol, the analysis environment, the name and version of the analysis tool based on the memo prepared at the time of the analysis, and so on.

Furthermore, since modification of digital data is possible and easy, this data may be rewritten by or during system operations. Therefore, it is necessary to preserve the data by ensuring that the data is identical to the original at the collection stage. This is the premise of data analysis. For example, it is necessary to ensure that a file downloaded from a server that is subject to investigation is identical to the file that was stored on the server.[117] For business operators to be able to preserve data, we believe that it would be useful for them to equip themselves with the capacities to suspend access to an account or file subject to investigation, to restore a deleted file, and to store the pre-modified version of a file, in response to investigating authorities' requests, to the extent that these functions will not impose an excessive burden. In addition, it also is advisable to preserve evidence, such as written depositions prepared by investigating authorities, using electronic signatures and time stamps.[118]

However, even if the courts attempt to confirm the records of the investigation process and examine investigating officials regarding the procedures used and custody of the data, courts may struggle to

---

115 Supreme Court, Decision, July 17, 2000, Keishu [*Supreme Court Criminal Case Report*], vol. 54, no. 6, p. 550 held the admissibility of the DNA examination result as evidence based on (i) the accuracy of the scientific theory and (ii) the scientific reliability of the implementation method. This framework applies not only to scientific evidence but to general evidence and also applies to data analysis (Go Naruse, *Admissibility of Scientific Evidence (Vol. 5: final)*, Hogaku Kyokai Manazine vol. 130, no. 5, pp. 1064-1065 (2013), Kohei Yoshimine et al., *Principles of Digital Forensics; Practice and Evaluation of Evidence*, Quarterly Keiji Bengo, no. 77, pp. 109-129 (2014)).

116 A hash value means a value of specific length with no regularity, which is the result of calculation using a certain calculation protocol applied to a file. SHA1 and SHA256 are commonly used calculation protocols.

117 If it is possible to confirm the hash values on the server of a business operator that provides cloud services subject to an investigation, the identification can be confirmed by checking these hash values with the hash values calculated regarding the file downloaded from the server. However, currently, there are no servers equipped with such a function. The following method can be considered an option: when several files having different sizes are uploaded on the subject server, and the hash values are calculated for each of these files after downloading these files, and if all the hash values are identical as a result of checking these hash values before uploading and after downloading the files, it can be confirmed that the subject server does not change the files at the time of download.

118 *See* Member Kubo's remarks in the minutes of the 4th meeting of the Criminal Law (pertinent to information and communications technologies) Subcommittee of the Legislative Council (https://www.moj.go.jp/content/001386019.pdf), p. 6.

evaluate the admissibility or probative value of data or analysis reports submitted as evidence because no criteria have been established for determining whether the process was appropriate. Therefore, we believe it is advisable to establish standards for digital forensic technologies in consultation with the interested parties and to revisit them as necessary in accordance with the evolution of technology.[119] In addition, we believe it will become important to expand the capabilities and systems by which courts themselves can evaluate the admissibility or probative value of data or analysis reports submitted as evidence.

3. Issues of Encrypted Data

In situations where investigating authorities have obtained encrypted data, different issues can arise depending on whether the subject who is compelled to provide access to the encrypted data is the suspect or a third party other than the suspect. We will consider the issues related to each of these scenarios separately.

(1) Relationship with Suspects

The right not to testify against oneself (privilege against self-incrimination; Article 38, paragraph (1) of the Constitution of Japan) may be an issue where an investigating authority compels a suspect to disclose a password for encrypted data or to decrypt encrypted data.[120]

There are U.S. court rulings in connection with this point. For example, in one case, when making a decision on whether the content of an investigating authority's request constituted an infringement of the privilege against self-incrimination, the ruling focused on whether the request compelled a person to externally express his/her thoughts.[121] In another case, the ruling focused on whether accepting the request itself had an element that constituted "testifying."[122]

In the United Kingdom, the Regulation of Investigatory Powers Act 2000 ("**RIPA**") provides that if the necessity, proportionality, and supplementary nature of disclosing a password are found, an

---

119 Commentaries on the accuracy of digital forensic analysis include the NPO Institute of Digital Forensics, *Guidelines for Preservation of Evidence: 9th Edition* (February 20, 2023) (https://digitalforensic.jp/wp-content/uploads/2023/02/shokohoznGL9.pdf), and Eitaro Hamuro & Kiyoshi Kuniura, *Introduction to Digital Forensics* (Tokyo Horei Publishing, 2015).

120 In cases where a suspect's face or fingerprint information is necessary to unlock a fingerprint authentication system or face authentication system, investigating authorities sometimes obtain such information by requesting a warrant to conduct a physical examination (Article 218, paragraph (1) of the Code of Criminal Procedure) with regard to the suspect.

121 *U.S. v. Doe*, 670 F.3d 1335, 1346 (11th Cir. 2012); Harumichi Yuasa, *Encryption and U.S. Constitution—Starting with the iPhone Issue*, Information Network Law Review vol. 15, pp. 96-101 (2017).

122 *Fisher v. U.S.*, 425 U.S. 391 (1976); *U.S. v. Doe*, 465 U.S. 605 (1984); *U.S. v. Hubbell*, 530 U.S. 27 (2000); Hiroki Sasakura, *Privilege Against Self-incrimination*, Hogaku Kyoshitsu, no. 265, pp. 103, 107-109 (2002); Tadashi Sakamaki, *One Aspect of Privilege Against Self-incrimination in the U.S.——Relationship with Document Production Orders——*; Kenji Hirose, Tatsuya Tada ed., *Commemorative Collection for Dr. Hitoshi Tamita Vol. 2*, pp. 447, 457 (Shinzansha, 2003).

investigating authority may compel a suspect to disclose the password subject to a certain judicial examination (Section 49(1) through (3), Section 50(1), Schedule 2 of the RIPA).[123]

Considering these examples in the U.S. and the United Kingdom, it can be expected that the issue of the relationship between the request that a suspect disclose a password or decrypt encrypted data and the privilege against self-incrimination will also be raised in Japan.[124]

(2) Relationship with Third Party Other Than Suspects

We assume that subjects who are third parties other than the suspect and who may be compelled to disclose a password or decrypt encrypted data would mainly be (i) business operators which store and keep encrypted data concerning the suspect and (ii) professional business operators possessing decrypting technologies.

For example, in the U.S., it is understood that investigating authorities may make a request for support for decryption to a person who has no direct relationship with the relevant suspect under the All Writs Act unless an unreasonable burden is imposed thereby.[125] In 2016, the FBI made a request under this act that Apple cancel the lock function of an iPhone, which led to a dispute.

In the United Kingdom, as with the case of a suspect, investigating authorities may compel a third party other than a suspect to disclose a password to these authorities or to decrypt encrypted data under the RIPA (Section 49(1) and Section 50(1) of the same act).

In Australia, as a result of the enactment of the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 in December 2018, investigating authorities can issue an order obliging a business operator to install a backdoor to access encrypted data held by it (Section 317E(1) and Section 317L of the same act).[126]

As shown above, there are currently various approaches internationally regarding whether a third party other than a suspect can be compelled to disclose a password or decrypt encrypted data and whether or

---

123 This is based on the idea that the privilege against self-incrimination under U.K. law applies where the subject information is not independent of the subject person's intention and relates to his/her thoughts, and it does not apply to a password that does not relate to someone's thoughts. However, some court precedents in the United Kingdom also suggest that there is room for considering that if knowledge of a password is a disadvantageous fact, such knowledge will be protected by the privilege against self-incrimination (Shotaro Maruhashi, *Disciplines for Decryption—Reference to Decryption Legislation in the United Kingdom* in *Commemorative Collection for the 70th Anniversary of the Birth of Professor Yoshihiro Hidaka (Second Half)*], pp. 393, 403-404 (Seibundo, 2018)

124 For example, Mr. Shigeki Matsui, a constitutional scholar, has pointed out that according to the current position of judicial precedents, it is highly likely that compelling disclosure of a password will not be deemed to constitute an infringement of the privilege against self-incrimination because a password itself is not information that constitutes self-incrimination (Shigeki Matsui, *Internet Constitutional Law: New Version*, p. 372 (Iwanami Shoten, 2014)). On the other hand, the Criminal Law (pertinent to information and communications technologies) Subcommittee of the Legislative Council raised an issue by pointing out that forcing a holder of crypto-assets to disclose the private key to the crypto-assets (if the holder refuses disclosure) constitutes an infringement of the privilege against self-incrimination (*see* Member Kubo's remarks in the minutes of the 6th meeting of the Criminal Law (pertinent to information and communications technologies) Subcommittee of the Legislative Council (https://www.moj.go.jp/content/001391536.pdf), p. 34).

125 *United States v. New York Tel. Co.*, 434 U.S. 159 (1977).

126 Australian Government, *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018, available at* https://www.legislation.gov.au/Details/C2018A00148.

not it is possible to make a request for cooperation by such third party. In Japan, it is necessary to engage in discussions with companies who have a stake in the matter, while paying attention to the developments in foreign jurisdictions. However, since obliging companies to install a backdoor in advance may be problematic from the viewpoint of the protection of human rights,[127] decreasing competitiveness of companies (in comparison with companies that are not obliged to install a backdoor), and the risk of information leakage due to misuse of backdoors, careful consideration of any of these measures is necessary before implementation.

The CLOUD Act does not oblige persons to decrypt data,[128] and an executive agreement cannot impose an obligation upon a government to compel a provider to decrypt encrypted data or to restrain a provider from decrypting such data in responding to an order from a foreign government.[129] Therefore, if highly encrypted data is uploaded onto a third party service and only users possess the decryption key, an issue arises as to whether that third party retains, stores, or controls the data; however, it is possible to imagine a situation where the third party does not have details about the users.[130] Further detailed discussions on responses to these situations are expected to take place in the future.

---

127 For example, issues may arise in relation to the secrecy of communications or right to privacy. Shigeki Matsui, *Internet Constitutional Law: New Version*, p. 379 (Iwanami Shoten, 2014) points out that disclosure of a decryption key will create an issue of freedom of expression.

128 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*, 5-6 (Apr. 2019), available at https://www.justice.gov/opa/press-release/file/1153446/download.

129 CLOUD Act Sec.105(a), 18 USC§ 2523(b)(3). A provision that seems to have a similar purpose is also contained in the "Agreement between Japan and the United States of America concerning Digital Trade" (Article 21, paragraph (3)).

130 Justin Hemmings et al, *Defining the Scope of 'Possession, Custody, or Control" for Privacy Issues and the CLOUD Act*, pp. 654-667.

V. Obtaining Data Stored Overseas for Investigative Purposes

We must also consider issues concerning the principles of international law, in addition to the issues concerning the access of data for purposes of investigation, when domestic investigating authorities seek data stored on a server located in a foreign state or managed by a foreign business operator or a domestic company operating in a foreign state.

1. Without Obtaining Consent of Foreign State, the Situs of the Server

When the data to be investigated is located in a foreign state, or if the subject data is managed by a foreign registered operator or by an entity that mainly operates its services abroad, one must also address whether any such access to foreign-held data for purposes of investigation constitutes a lawful exercise of jurisdiction under international law.

(1) The Concept of Jurisdiction and Issues to Be Addressed Regarding International Law

A. Jurisdiction and Standards of Conduct

When Japanese investigating authorities seek data stored on foreign servers for purposes of investigation, the territorial scope of Japan's Code of Criminal Procedure is understood to include the countries where such servers are located.[131] However, questions remain as to whether such conduct infringes upon the sovereignty or jurisdiction of other foreign states.[132]

In order for a country to enact, apply, or enforce domestic law (be it over individuals, assets, or matters/activities), a country must have "national jurisdiction" over the relevant circumstance.[133] This "national jurisdiction" is divided into three sub-concepts: (i) legislative jurisdiction, which authorizes a legislative body to enact a domestic law or regulation as criteria for recognizing the legality of certain phenomena and activities subject thereto; (ii) enforcement jurisdiction, which authorizes a judicial or executive body to enforce domestic laws and regulations by means of arrest, search, forcible examination, seizure, detention, etc.; and (iii) judicial jurisdiction, which authorizes a judicial body or administrative tribunal to define the scope of jurisdiction to exercise the judicial power, to try a specific case, and to render a decision by applying domestic laws and regulations.[134]

---

131 Despite the code's inherent perspective on extraterritorial applicability, the prevailing view amongst academics and practitioners is the so-called "foreign sovereignty-restrictive theory," which states that extraterritorial application of one country's law should be subject to restrictions born of the relevant foreign country's sovereignty (Yoshimitsu Yamauchi, *Investigation Activities Overseas*, in Koya Matsuo and Toru Iwase, *Exemplified Code of Criminal Procedure I*, pp. 5 and 10-12 (Seirin Shoin, 2012); Junichi Yoshikai, Hankai Jurist, no. 1562, pp. 98, 100 (2021)).

132 Council of Europe Cybercrime Convention Committee (T-CY), *Transborder access and jurisdiction: What are the options?,* Doc no T-CY (2012)3, 6 (2012) *available at* https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e79e8.

133 Soji Yamamoto, *International Law (New Edition)*, p. 231 (Yuhikaku Publishing, 1994); Yuji Iwasawa, *International Law*, p. 174 (University of Tokyo Press, 2020).

134 Hironobu Sakai et al., *International Law*] p. 85 (Yuhikaku Publishing, 2011); Akira Kotera, *Conceptual Classification of Extraterritorial Jurisdiction of National Jurisdiction* in Commemorative Collection for the 70th Anniversary of the Birth of Soji Yamamoto, *National Jurisdiction: International Law and Domestic Law*], pp. 343 and 343-344 (Keiso Shobo 1998); Akira Kotera et al. (ed.), *Lecture on International Law* (2d edition), p. 163 (Yuhikaku Publishing 2010); Yuji Iwasawa, *International Law*, pp. 174-175 (University of Tokyo Press, 2020).

Whether a country has the aforementioned types of jurisdiction over a particular circumstance is determined in accordance with established principles of international law, such as the "territoriality" and "nationality" principles.[135] In addition, some consider that a "substantial and genuine connection"[136] between a particular country and the relevant circumstance may form a basis for the exercise of jurisdiction.

The most widely accepted basis of jurisdiction accepted by international law is the territoriality principle,[137] since states have the closest connection with persons and actions within their territory.

Notwithstanding the above, due to the expansion of transboundary economic activities after World War II, certain states started to apply their public interest-oriented regulations extraterritorially. A conspicuous example is judicial friction involving the U.S. government's extraterritorial application of its antitrust law. In the 1945 *Alcoa* case[138] the federal court relied its decision on the so-called "effects doctrine" which allows the application of U.S. antitrust law to cartel conduct performed by a foreign national in a foreign state if such conduct has an anti-competitive effect within the U.S. and if that effect was intentionally produced. Subsequently, the effects doctrine has allowed many cases of extraterritorial application of U.S. antitrust law. Incidental to those U.S. domestic court proceedings, the U.S. investigating authorities have performed enforcement measures, such as issuing document-production orders to foreign companies and conducting investigatory interviews outside U.S. territory. In opposition to this U.S. practice, European countries enacted "blocking statutes" to prohibit domestic business entities and individuals from disclosing information to foreign authorities, hampering the efforts of U.S. authorities' evidence collection activities to a certain extent.[139]

Nonetheless, the effects doctrine subsequently became international practice. Canonization of this sentiment is somewhat reflected in the fourth Restatement of the Foreign Relations Law of the United States, which indicates that a "genuine connection" between a country and the relevant circumstance serves as a more generalized basis for the exercise of jurisdiction and notes elements of territorial jurisdiction, personality jurisdiction, and effects-based jurisdiction as conventional *prima facie* grounds.[140]

Moreover, it appears to be widely acknowledged, not only in the U.S., that under the current principles of international law, in order for a state to legitimately exercise its national jurisdiction, there should be a "justifiable connection" between the state and the subject (such as a company) being regulated. However, in order to determine what constitutes a "justifiable connection," we must examine state practice. In this respect, the following examples form the basis and define the scope of jurisdiction under some domestic laws: when the relevant company is subject to that country's jurisdiction; when a

---

135 Hironobu Sakai et al., *International Law*, p. 86 (Yuhikaku Publishing, 2011); Yuji Iwasawa, *International Law*, pp. 175-183 (University of Tokyo Press, 2020).

136 Soji Yamamoto, *International Law (New Edition)*, p. 234 (Yuhikaku Publishing, 1994).

137 Soji Yamamoto, *International Law (New Edition)*, p. 239 (Yuhikaku Publishing, 1994).

138 *United States v. Aluminum Co. of America*, 148 F.2d 416 (1945).

139 For extraterritorial application of U.S. antitrust law and each country's opposition legislation, *see* Yurika Ishii, *International Regulation of Cross-border Crimes*, p. 137-160 (Yuhikaku Publishing, 2017).

140 Restatement (Fourth) of the Foreign Relations Law of the United States§ 407-413 (AM. LAW INST. 2018).

substantial number of users of the relevant company exist within the territory of the state; and when the relevant company's services target the consumers of that state.[141]

---

[141] For example, under the CLOUD Act, a service provider subject to U.S. jurisdiction can be ordered to disclose data managed, controlled, or held by such service provider, whether the data is stored domestically or overseas.

Elements to consider when assessing whether or not a particular service provider is subject to U.S. jurisdiction are: (i) whether the service provider is located (e.g., a business office) within the U.S., or absent such physicality; (ii) whether the service provider located outside the U.S. provides services targeted to U.S. users, considering the nature, volume, and quality of the services (for example, whether its website displays content dedicated to U.S. users.). (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*, 8 (Apr. 2019), *available at* https://www.justice.gov/opa/press-release/file/1153446/download).

Furthermore, as stated in **III.1.(2)** above, the proposed EU Electronic Evidence Regulation and Directive ensure the effective exercise of jurisdiction by obligating service providers not established in the EU member states but offering services in the territory thereof to designate at least one legal representative in the EU, and that an order to disclose data located within and outside the EU territory and other measures be addressed to that legal representative, who is present in the EU.

Article 2-2 of the Telecommunications Business Act of Korea authorizes extraterritorial application, providing that "This Act shall apply to any conduct committed overseas when such conduct affects the Korean market or users in the market." Specifically, Article 87 of the same act provides that when a business operator without a business office in Korea provides basic telecommunications services, such as telecommunications services using telecommunication line facilities, to users within Korea from outside Korea such business operator must enter into an "agreement" regarding cross-border provision of basic telecommunications services, with a basic telecommunications business operator located within Korea that similarly provides basic telecommunications services. The Act also requires that the business operator comply with certain domestic statutory provisions when providing cross-border basic telecommunications services pursuant to that "agreement." Article 87 also applies to Article 83 of the same act, which results in a business operator without a business office in Korea having to comply with an order from Korean investigating authorities to submit certain information, such as names, resident registration numbers, addresses, telephone numbers, IDs, and the dates of commencement of use of the services by users of the relevant telecommunications business (Telecommunications Business Act (Act No. 16019; Latest revision: December 24, 2018), *available at* http://www.law.go.kr/lsInfoP.do?lsiSeq=206000&efYd=20190625#J2:2 (Korean text only)). In addition, Article 32-5 of the Korean Information Communication Network Act requires an information communication service provider to appoint an agent acting in Korea, when that service provider does not have an address or business office in Korea, provides information communication services to Korean users, and has a certain level of sales. Article 64 of the same act obligates such agent set in Korea to submit information in situations such as when an action violates the same act or when an incident or accident significantly impairs the assurance of users' safety and trust (Act on Promotion of Use of Information Communication Network and Information Protection (Act No. 16021, Latest Revision on December 24, 2018), *available at* http://www.law.go.kr/lsInfoP.do?lsiSeq=206009&efYd=20190625#0000 (Korean text only); For factors determining whether the relevant business operator provides information communication services aimed at Korea, *see* Korean Broadcast and Communications Committee, *Guide on Designating a Domestic Representative in Korea* (March 2019) (*available at* https://kcc.go.kr/download.do?fileSeq=48880)).

However, the question still remains whether such mandatory appointment of a domestic representative under domestic law is in accordance with international agreements regarding trade in services and e-commerce.

B. Cyberspace and Sovereignty

As for the relationship between cyberspace and sovereignty, the Tallinn Manual 2.0[142] which sets out international legal principles and rules regarding cyberspace activities provides the following: namely, whilst acknowledging that states enjoy sovereignty over any cyber infrastructure (such as cables, routers, servers, personal computers) located in their territory, and over any operations of that cyber infrastructure,[143] the manual debates whether or not a country's remote cyber operations could be considered to violate the sovereignty of a foreign state based on: (i) the degree of infringement upon the target State's territorial sovereignty and integrity, and (ii) whether there has been interference with or usurpation of an inherently governmental function. Examples include a particular country's government officials conducting cyber operations while physically present in another State's territory, and physical damage or lost functionality of cyber infrastructure located in another State caused by remote cyber activities.[144]

(2) International Law Assessment of Accessing Overseas Data for Investigative Purposes

As stated in **V.1.(1)B**, each country enjoys sovereignty over IT infrastructures located within its territory as well as operations of those infrastructures. Therefore, when accessing data stored in another state, it begs the question whether this action is tantamount to unlawful exercise of jurisdiction infringing the other state's sovereignty and jurisdiction.

First and foremost, if a state exercises its sovereign acts in the territory of another country, absent that country's consent, the acting state violates the other state's territorial sovereignty, and the act is prohibited under international law. Hence, a state's investigating authorities may not physically enter the territory of another state in order to access data located within another state for investigative purposes. Such actions by an investigating authority would constitute the enforcement of jurisdiction within the territory of another state, and thus would violate the territorial sovereignty of another state, which is impermissible under international law.

In addition, when an investigating authority obtains data stored on a server located overseas via electronic network, even though the investigating authority does not physically enter the foreign state's territory, since there is a possibility of violating the foreign state's sovereignty, the question of how such investigation should be assessed under international law still remains.

---

142 Michael N. Schmitt's Tallinn Manual 1.0 on the International Law Applicable to Cyber Warfare (2013) was published by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defense Centre of Excellence, and discusses whether the most severe cyber operations violate the prohibition of the use of force in international relations, or entitle states to exercise the right of self-defense under international law. The Tallinn Manual 2.0, which was published in 2017, discusses assessments of more common cyber incidents which fall below the thresholds of the use of force or armed conflict, from the perspective of various areas of international law.

143 Michael N. Schmitt, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, 11 (2d ed. 2017). Cyberspace has also been described variously as a "global domain" or "fifth domain." that lacks physicality and is virtual in nature. It is also sometimes suggested that it should be likened to the high seas, international airspace, or outer space in the sense of constituting a "global commons" (*res communis omunium*). However, the Tallinn Manual 2.0 acknowledges that national sovereignty extends to cyberspace, since cyber activities occur in territory and involve objects, or are conducted by persons or entities, over which States may exercise their sovereign prerogative (*ibid*. 12).

144 Michael N. Schmitt, TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS, 17-21 (2d ed. 2017).

A. Seeking Data Submission from Server-Managing Entities

Investigating authorities' access to data stored overseas via data production orders issued to a server-managing entity can take the form of either (i) an order by the investigating authorities to the relevant domestic company to submit data stored in a foreign country (e.g., seizure via an order to produce copies of records, as described in **IV.1.(1)**),[145] or (ii) a direct order from investigating authorities to foreign server-managing entities to submit data held by those foreign operators located in a foreign state. They can be analyzed under international law as below.

With respect to (i), if the server managing entity that is the subject of the data/data-medium production order is located within the ordering country, that country has clear enforcement jurisdiction over the sever managing entity based on the territoriality principle. Moreover, as for the data stored in a server located overseas, if the data is accessed by a managing entity located within the ordering country's territory which received a production order, and the actual act of obtaining and producing the data in question or the recording medium containing such data is done in the territory of the ordering state, as such this should be permitted under international law; this differs from enforcement measures

---

145 As stated in **IV.1.(1)**, in Japan, a "seizure via an order to produce copies of records" is a system that enables investigating authorities to order a company located in Japan to submit data stored in a foreign country. The legislators of this system expressed their view that the act of accessing a foreign server and recording data is carried out by a private individual (within the managing authority, not the government) subject to the relevant order and, therefore, does not constitute an infringement of the sovereignty of that foreign country (Noriaki Sugiyama & Masayuki Yoshida, *Act for the Partial Amendment of the Penal Code to Respond to the Advancement of Information Processing (Second Half)*, Hoso-jiho, vol. 64, no. 5, pp. 55, 74 (2012)).

Another view, casting doubt on the logic used when concluding that Remote Access does not constitute an infringement of sovereignty, is that insofar as data is recorded pursuant to an order issued by an investigating authorities, that recording action, including accessing data located in a foreign country, is part of the investigating authorities' conduct (Toshihiro Kawaide, *Computer Network and Cross-border Investigations* in *Commemorative Collection for the 70th Anniversary of the Birth of Professor Masahito Inoue*, pp. 409 and 414 (Yushikaku Publishing, 2019)). In addition, in the Microsoft Case, which is considered to be the genesis of the CLOUD Act, it was held that many countries, including Ireland where the relevant server was located, agreed with Microsoft's assertion that the investigative technique in question was problematic in that it would give rise to a situation where all countries would be able to obtain data of interest to them, irrespective of the place of data storage, solely because they have jurisdiction over the entities which have the technical ability to obtain and produce the subject data. (Currie, Robert J., *Cross-Border Evidence Gathering in Transnational Criminal Investigation: Is the Microsoft Ireland Case the "Next Frontier"?*, 54 Canadian Yearbook of International Law 63, 87-89 (2017)).

whereby an investigating authority physically enters the territory of another state to conduct investigations and enforce their jurisdiction.[146]

In this respect, the Japanese Companies Act requires that a Foreign Company (as defined in Article 2, item (ii) of the Act) that intends to carry out transactions in Japan on a continuing basis must specify representatives in Japan (Article 817, paragraph 1 of the Companies Act) and complete registration as a Foreign Company (Article 818, paragraph 1 of the Companies Act). Furthermore, the Japanese Telecommunications Business Act requires that a foreign corporation or other entity[147] to which the Japanese Telecommunications Business Act applies must designate a domestic representative or domestic agent and provide notice thereof to the Minister for Internal Affairs and Communications when applying for registration of or making a notification concerning the telecommunications business (Article 10, paragraph 1, item (ii) and Article 16, paragraph 1, item (ii) of the Telecommunications Business Act). Whether or not a framework should be created, pursuant to which business operators outside of Japan are required to submit data stored abroad through their representatives or agents (or whether it would be appropriate to use another framework) is precisely the kind of question that needs to be considered in light of the issues described in this report.

---

146 With regard to the issue of whether it is permissible to issue an order to submit data stored in a foreign country to a domestic business entity without the consent of the country where the data is located, although one source takes a negative view (Bert-Jaap Koops & Morag Goodwin, Cyberspace, *the Cloud and Cross-Border Criminal Investigation: The Limits and Possibilities of International Law,* Tilburg: Tilburg Institute for Law, Technology and Society, 61-62(2014)) many academics regard the issue in a positive manner. (For an opinion that expressly approves the permissibility of such requests, as part of a general discussion of extraterritorial application, *see* Mann, Frederick Alexander, *Doctrine of International Jurisdiction Revisited after Twenty Years*, 186 Recueil des Cours 9, 47-49 (1984). For an opinion that there are no unified state practices on this issue, *see* Currie, Robert J., *Cross-Border Evidence Gathering in Transnational Criminal Investigation: Is the Microsoft Ireland Case the "Next Frontier"?*, 54 Canadian Yearbook of International Law 63, 83 (2017).) In addition, as mentioned in footnote 141 above, it seems to be a practice trend among some countries, such as Korea and the EU member states, to require a service provider to establish an agent or base facility within the relevant country's own territory and then to order that agent or base facility to obtain or submit data stored in foreign countries. In practice, there seems to be many countries other than Japan that actually request domestic persons or entities authorized to use foreign located servers to submit data (or a recording medium containing the data) stored thereon, without using MLATs, and correspondingly, many companies that receive such requests (Currie, Robert J., *Cross-Border Evidence Gathering in Transnational Criminal Investigation: Is the Microsoft Ireland Case the "Next Frontier"?*, 54 Canadian Yearbook of International Law 63, 91-93 (2017)). In addition, the Belgian Court of Cassation issued a decision permitting the submission of an order for data stored outside of Belgium (*Yahoo!*, Hof van Cassatie van België, 1 December 2015, Nr. P.13.2082.N. (unofficial English translation, http://journals.sas.ac.uk/deeslr/article/viewFile/2310/2261)). Furthermore, it is possible that data stored in a foreign country may be subject to a data production order under Article 18 of the Convention on Cybercrime (*see* **2.(2)A** below).

147 On February 12, 2021, the Ministry of Internal Affairs and Communications changed its previous interpretation of the geographic coverage of the Telecommunications Business Act, and indicated its view that Telecommunications Business Act applies to foreign corporations and other entities where the foreign corporation or other entity "operates a telecommunications business that involves providing telecommunications services within Japan" or "operates a telecommunications business that involves providing telecommunications services to persons within Japan from overseas" (the Ministry of Internal Affairs and Communications, *View on the Application of the Telecommunications Business Act when Foreign Corporation or Other Entity is Operating Telecommunications Business* (February 12, 2021)(https://www.soumu.go.jp/main_content/000739291.pdf)).

On the other hand, with regard to (ii), when an ordering country's investigating authorities directly request a server-managing entity, which is located in a foreign country, to submit data, the ordering country is understood to have legislative jurisdiction over the server-managing entity if there is a "justifiable connection" between the ordering country and the managing entity, such as where the managing entity actively provides services to users in the ordering country; however, separate and careful assessment under international law would be required to make a determination with regard to whether the ordering country has enforcement jurisdiction over the server-managing entity. To this end, due to the absence of any concrete international principle on the legality of enforcement jurisdiction in such cases, it is important for states to establish a multilateral consent mechanism that ensures that directly seeking data from extraterritorial managing entities does not violate the sovereignty of foreign states.

B. Acquiring Data Through Direct Access to a Server Located in a Foreign Country

How should international law evaluate trans-border data investigations in which an investigating authority attempts to obtain data by directly accessing a server located in a foreign country, as in the case of Remote Access Under the Code of Criminal Procedure of Japan?

Exercise of jurisdiction in another country's territory constitutes an infringement of territorial sovereignty if the relevant action is deemed to be a usurpation of the sovereign authority of relevant nation-state,[148] except where permitted pursuant to international custom or treaty.

Remote Access is an investigative method employed from within investigative countries which involves the use of existing network protocols and legally obtained (i.e. pursuant to applicable regulations, such as criminal procedural law) credential information (e.g., user ID, password, etc.) to directly obtain data stored overseas. Even when the location of the server on which the targeted data is stored is unknown, and there is a possibility that the server is located in another foreign country, Remote Access does not involve an investigating authority physically entering into a foreign country. Due to this absence of physical presence of the investigating authority in a foreign country, it could be said that Remote Access does not constitute enforcement measures enforcing the jurisdiction "in the

148 S.S. Lotus (France v. Turkey), 1927 P.C.I.J. (ser. A) No. 10 at 18-19 (Sep. 7); Michael Akehurst, "Jurisdiction in International Law," 46 BRITISH YEAR BOOK OF INTERNATIONAL LAW,146, 147 (1972).

territory of a foreign country." However, as a matter of international law, opinions on this issue are divided.[149] [150]

Therefore, as mentioned in **V.2(2)** below, in light of the need for such trans-border investigation of foreign stored data, during the deliberation stage, the Second Additional Protocol to the Convention of Cybercrime sought to justify, under international law, investigative methods that enable investigating authorities to obtain data through direct access to servers located in foreign countries, without limiting themselves to the conventional principles of territorial sovereignty. However, the point was not negotiated due to a lack of time for agreement within the designated timeframe (*see* **2.(2)B** below).

Meanwhile, discussions on Remote Access to servers located in foreign countries also have progressed in Japan in recent years.

In Japan, while the legislators who introduced Remote Access under the Code of Criminal Procedure found that there is no internationally accepted common view as to whether accessing a server located in a foreign country infringes on that country's sovereignty, they are of the view that investigating authorities should refrain from conducting Remote Access involving a server that clearly is located in

---

149 Currie, Robert J., *Cross-Border Evidence Gathering in Transnational Criminal Investigation: Is the Microsoft Ireland Case the "Next Frontier"?*, 54 CANADIAN YEARBOOK OF INTERNATIONAL LAW 63, 76-80 (2017). Some countries explicitly permit Remote Access to data stored in a foreign country under their domestic laws or regulations. For example, the Belgian Criminal Procedure Code allows duplication of data stored in a foreign country under certain circumstances (Code d'Instruction Criminelle, Art. 88 ter). Furthermore, in the U.K., although there is no statute, Sections 19-20 of the Police and Criminal Evidence Act 1984 are interpreted to permit Remote Access to data stored in a foreign country. *See* also, European Judicial Cybercrime Network, "Country information on direct access to e-evidence" (https://www.eurojust.europa.eu/judicial-cooperation/practitioner-networks/european-judicial-cybercrime-network).

There are also foreign court decisions permitting Remote Access to data stored in a foreign country. Examples include: a court decision allowing a Korean investigating authorities' Remote Access to data storage media located in a foreign country (Korean Supreme Court, Judgment, November 29, 2017 (2017, 9747) (Korean text: https://www.scourt.go.kr/sjudge/1512108215099_150335.pdf; English translation: http://library.scourt.go.kr/SCLIB_data/decision/20_2017Do9747.htm)), and a Norwegian court decision that permitted a Norwegian investigating authority to download data stored in a foreign country from data terminals located in a domestic company office (Tidal Music AS v. The public prosecution authority, 28 March 2019, HR-2019-610-A, (case no. 19-010640STR-HRET) (English translation: https://www.domstol.no/globalassets/upload/hret/decisions-in-english-translation/hr-2019-610-a.pdf)); a case permitting Danish investigating authorities to access an SNS account (U 2012.2614 H, Højesteret, 12.05.2012)(unofficial translation:https://sas-space.sas.ac.uk/5563/1/2038-2939-1-SM.pdf).

150 Recently, it has become more common for companies to simply not disclose the location(s) of their servers, and also for companies to intentionally conceal the location of their server(s) by causing users to use the dark web. One question with regard to these practices is whether it is permissible to issue a warrant authorizing Remote Access when the location of the relevant server is unknown. One view is that issuance of such a warrant is permissible, even though it has not been confirmed that the relevant server is located within the investigating country. Another view states that the consent of the relevant foreign country should not be a requirement for issuance of such warrants (Hiroshi Kawamura et al., *Outline of Cybercrime—Legal Commentary and Actuality of Investigation and Public Trial*, p. 157 Yoshihiro Ohara and others (Seirin-Shoin, 2018); Hiroki Sasakura, *Cloud Investigation*, in Kuniji Shibahara et al., *Economic Criminal Law – Practice and Theory*, p. 571 (Shojihomu, 2017); Haruki Sugiyama, *Limitation of Investigation Activities in Foreign Countries*, in Ryuichi Hirano & Koya Matsuo, *New Exemplified Criminal Procedure Law I* pp. 55-56 (Seirin-Shoin, 1998)). In fact, U.S., Rule 41 of the Federal Rules of Criminal Procedure authorizes the issuance of a warrant for cross-border Remote Access in situations where the location of data is kept secret by technological means.

a foreign country and, instead, rely on international assistance in investigations.[151] However, in Japanese academia, it has been noted that it would become impossible for investigating authorities to continue their investigations if it is necessary to resort to international assistance in investigations even in situations where the location of the server is unknown; therefore, investigating authorities should be permitted to conduct Remote Access immediately in such situations, and if it later becomes apparent that the server is located in a specific foreign country, the previous Remote Access should not become retroactively unlawful.[152] Others cast doubt on the view that Remote Access is an infringement of sovereignty, noting that accessing a server located in a foreign country should be differentiated from physical entry into the territory of a foreign country.[153]

Given this, the 2021 Japanese Supreme Court Decision ruled as follows: if (i) "a recording medium that stores electromagnetic record is located in a country that is a signatory to the Convention [on Cybercrime]," and (ii) "the lawful and voluntary consent of the person who has lawful authority to disclose the records has been obtained, both Remote Access to the recording medium and copying of the records are permitted without resorting to international assistance in investigation." However, the 2021 Supreme Court Decision is considered to have merely ruled on whether there was any "material illegality" in the evidence collection procedure, as a premise for determining whether evidence collected by Remote Access would be excluded as illegally collected evidence,[154] and therefore, it does not appear to specify criteria for determining the legality or illegality of Remote Access.

While the 2021 Supreme Court Decision clearly states that Remote Access that satisfies both requirements (i) and (ii) above is legal, it does not clearly opine on the legality of Remote Access that does not satisfy one or both of these requirements. However, with regard to the Remote Access that was at issue in the 2021 Supreme Court Decision, the court stated that even though the access did not satisfy requirement (i) (specifically, the whereabouts of the recording medium that stored the electromagnetic record was unknown), "it cannot be said that it was unreasonable for police officers to adopt a policy to perform Remote Access (and other matters), with the voluntary consent of persons related to Y without resorting to international assistance." It is possible that the Supreme Court opinion is based on the premise that Remote Access may be performed legally as long as requirement (ii) above is satisfied even if requirement (i) is not.[155] Furthermore, the 2021 Supreme Court Decision upheld the admissibility of the evidence collected via Remote Access ("Procedure <B>") of which there was no denial of voluntary approval by the person subject to the relevant disposition, based on an extremely brief rationale; it is possible that the court opinion is based on the premise that

---

151 *177 Sessions of the Diet, Minutes of Judicial Committee Meeting of the House of Representative, No. 14* (May 27, 2011), p. 10 (Answer of Minister of Justice Satsuki Eda); Noriaki Sugiyama & Masayuki Yoshida, *Act for the Partial Amendment of the Penal Code to Respond to the Advancement of Information Processing (Second Half)*, Hosojiho, vol. 64, no. 5, pp. 100-101 (2012).

152 Toshihiro Kawaide, *Computer Network and Cross-border Investigations* in *Commemorative Collection for the 70th Anniversary of the Birth of Professor Masahito Inoue*, pp. 428-429 (Yushikaku Publishing, 2019).

153 Yoshimitsu Yamauchi, *Case finding material illegality in the investigation that connected a personal computer seized pursuant to a search warrant to a mail server located overseas and excluding evidence* Kenshu, no. 832, pp. 13 and 22-25 (*Shiyukai Secretariat & Kenshu Editorial Staff*, 2017).

154 Junichi Yoshikai, Hankai Jurist, no. 1562, pp. 98, 104 (2021).

155 Go Naruse, Hanhi Jurist, no. 1577, pp. 160, 163 (2022).

there are fewer problems under the Code of Criminal Procedure in the case of Remote Access implemented as a voluntary disposition.[156]

Furthermore, possibly in light of the trend indicated by the 2021 Supreme Court Decision, a dissertation by the then-Senior Attorney for International Affairs of the Criminal Affairs Bureau of the Ministry of Justice published as a personal opinion in November 2022 (after the 2021 Supreme Court Decision), expresses the view that "Remote Access with the lawful and voluntary consent of the person who has the lawful authority to disclose the electromagnetic record is permissible [regardless of the country where the server is located]," and also states, with respect to Remote Access via a compulsory measure based on a warrant, this is permissible "if it is difficult to discern whether there is a need to demand international assistance in the investigation and to which country the demand should be made.[157] It is believed that this opinion presents the basic guideline for Japanese investigating authorities to perform Remote Access to servers located in a foreign country through a person located in Japan.

However, as indicated by, among others, Osaka High Court, Judgement, September 11, 2018, Keishu [*Supreme Court Criminal Case Report*] vol. 75, no. 2, p. 2020 (the original judgment in the 2021 Supreme Court Decision), because courts tend to construe the existence of voluntary approval narrowly, it might not necessarily be desirable from the perspective of promptness and stability of investigations to prioritize obtaining the approval of the person who has access authority and perform an investigation entirely in reliance on this. In addition, when engaging in Remote Access, consideration should be given not only to the Data Subject, but also to the interests of the entities responsible for managing servers on which data is stored (*see* **IV.1.(3)B(b)** above), but it may not be possible to consider the interests of server-managing entities adequately when proceeding with Remote Access as a voluntary investigation based on the approval of the person with access authority.[158] Accordingly, in the mid- to long-term, one conceivable alternative would be to attempt

---

156 The supporting opinion of Judge Miura also states, with regard to the admissibility of [evidence] collected by the Remote Access in question that it "should be determined by taking into consideration the existence of voluntary approval of the person with authority, and other various factors found in relation to the relevant procedure" (emphasis added), and possibly suggests that there are few issues in situations involving Remote Access performed as a voluntary disposition.

157 Ryozo Kitajijma, *Cross-border Remote Access*, Keisatsugaku Ronshu, vol. 75, no. 11, pp. 114, 134-138 (2022).

158 Furthermore, as stated in footnote 55 above, data stored on a company server contains various types of highly private information, and considering that the situation is similar to privacy in a residence, it might be desirable to enhance due process with regard to the person with access authority also.

to form an agreement to allow international cross-border Remote Access directly under international law, with due process secured by examination for a warrant.[159] [160]

(3) Coordination of Conflicts Among the Laws of Countries

In situations where data is to be obtained for investigative purposes from a server located in a foreign country, in addition to issues concerning infringement of sovereignty or jurisdiction as discussed in **(1)** and **(2)** above, another problem may arise. Namely, whether the manner of obtaining data referenced above is subject to any restrictions under international law because of conflicts with procedural safeguards that protect individual rights (the individual countries' data protection laws, personal information protection laws, etc.). For example, the EU has indicated, at an early stage, that transferring personal data to the U.S. by accepting a disclosure order under the CLOUD Act conflicts with the cross-border transfer restriction (Article 48) of the GDPR. Thus, the European Parliament once claimed that the procedural and other aspects established in the CLOUD Act did not conform to the GDPR and recommended the suspension of the EU-US privacy shield.[161] Then, following the decision of the European Court of Justice on July 16, 2020 that invalidated the EU-US privacy shield, on October 7, 2022, the U.S. published a new EU-US data privacy framework (EU-U.S. Data Privacy Framework; the "**DPF**"), that allegedly addressed all of the concerns raised by the decision and is based on an Executive Order issued by the U.S. President and regulations provided by the Attorney

---

159 A journal article by the then-Deputy Director-General of the International Legal Affairs Bureau of the Ministry of Foreign Affairs, published as a personal opinion in May 2022 expresses the following view: "there seems to be a certain rationale in the following statement as to the way to balance the domestic need for a criminal investigation and the consideration to be given to another country's territorial sovereignty: while it may be difficult to immediately form an international agreement, from a mid- to long-term perspective, … if a person with legitimate access authority is located in Japan, and the investigating authority merely accesses, refers, and photocopies that data over which the person has legitimate authority, with a warrant where needed by the investigating authority for criminal investigation, … it highly likely that basically the act will not constitute an illegal infringement of sovereignty" (emphasis added) (Tomohiro Mikanagi, *The Function of Territorial Sovereignty in International Rules Governing the Use of the Internet*, Kokusai-ho Gaiko Zassi [The Journal of International Law and Diplomacy] vol. 121, no. 1, pp. 1, 14 (2022)).

160 This direction also is consistent with the OECD Government Access Declaration, which requires that prior approval and oversight mechanisms should be established in relation to government access (*see* **Column (i)** above).

161 European Parliament, *Adequacy of the protection afforded by the EU-US Privacy Shield Europe an Parliament resolution of 5 July 2018 on the adequacy of the protection afforded by the EU-US Privacy Shield*, 2018/2645(RSP), *available at* http://www.europarl.europa.eu/doceo/document/TA-8-2018-0315_EN.pdf. Moreover, a joint answer from the European Data Protection Superviso r (EDPS) and the European Data Protection Board (EDPB), addressed to European Parliament's Committee on Civil Liberties, Justice and Affairs (LIBE Committee), indicates that transfers of personal data to the U.S. based on the CLOUD Act conflicts with Article 48 of the GDPR an d emphasizes the importance of the EU and the U.S. entering into a comprehensive agreement regarding access to electronic evidence. (EDPB, *EDPB-EDPS Joint Response to the LIBE Com mittee on the impact of the US Cloud Act on the European legal framework for personal data protection*, (12 July, 2019), *available at* https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-edps-joint-response-libe-committee-impact-us-cloud-act_en).

General.[162] The DPF clarifies that: data that can be subject to an order from the U.S. is limited to that which is necessary and proportionate; EU individuals will be able to lodge a complaint concerning a demand by the U.S. with the "Civil Liberties Protection Officer" (the "**CLPO**") of the U.S. intelligence agency, and the CLPO will submit the results of its investigation to the Attorney General for appropriate measures to be taken (the Attorney General will work with the Foreign Intelligence Surveillance Court); EU citizens may appeal the CLPO decision to the U.S. Data Protection Review Court (comprised of three judges independent from the U.S. government), and that court may conduct necessary investigations and render an order to delete the data. Deliberations on the adequacy decision by the EU are expected to progress in the future.[163] Similar issues also might arise with respect to relationships with other countries.[164]

However, in principle, each country has discretion to determine what laws to enact within the scope of its legislative jurisdiction. How to coordinate conflicts between a Data Production Order by a certain country with domestic laws remains unclear, and it is hard to say that there are any established international legal principles on this issue.[165]

The U.S. uses, as a matter of domestic law, comity based on the balancing of interests of the sovereign powers concerned. Actually, as stated in **III.1.(2)** above, the CLOUD Act provides that if certain requirements are met, a provider subject to a data disclosure order may file a motion to quash or modify the order with a U.S. court, and that U.S. courts should consider comity in ruling on those motions.[166] Comity, as a matter of general international law, cannot escape from ambiguity that may arise in the rendering of a judgment based on comity, and issues remain as to whether or not a problem exists with comity judgments from the perspective of foreseeability and as to whether or not comity judgments tend to be favorable to the rendering country. Under the CLOUD Act, certain responsive measures are attempted by stipulating specific factors to consider in rendering a comity judgment.

---

162 The White House, *FACT SHEET: President Biden Signs Executive Order to Implement the European Union-U.S. Data Privacy Framework*, (October 7, 2022), *available at* https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/07/fact-sheet-president-biden-signs-executive-order-to-implement-the-european-union-u-s-data-privacy-framework/. In response to the foregoing, on December 13, 2022, the European Commission commenced the process toward adoption of adequacy certification for the DPF, and published the draft decision (European Commission, *Data protection: Commission starts process to adopt adequacy decision for safe data flows with the US* (13 December 2022), *available at* https://ec.europa.eu/commission/presscorner/detail/en/ip_22_7631), with a view to being certified in around the summer of 2023. Other than the foregoing, on January 11, 2023, the U.S. Department of Commerce published Q&As concerning the DPF (https://www.privacyshield.gov/article?id=EU-U-S-Privacy-Shield-Program-Update).

163 EDPB, *DEBB welcomes improvements under the EU-U.S. Data Privacy Framework, but concerns remain*, (28 February, 2023), *available at* https://edpb.europa.eu/news/news/2023/edpb-welcomes-improvements-under-eu-us-data-privacy-framework-concerns-remain_en.

164 For data protection laws and regulations and personal information protection laws of other countries, including [information on] the existence and details of any procedural safeguards to protect individuals' rights, *see also*, Nishimura & Asahi, *Report on the results of a survey of systems for the protection of personal information in foreign countries*, (November 2021)(https://www.ppc.go.jp/files/pdf/offshore_DPA_report_R3_12.pdf).

165 Hironobu Sakai et al., *International Law*, p. 86 (Yuhikaku Publishing, 2011). *See also*, The European Union and the Council of Europe, *Cooperation between law enforcement and Internet service providers against cybercrime: towards common guidelines,* p. 5 (2020), *available at* https://rm.coe.int/0900001680a091a7.

166 CLOUD Act, Sec.103(b), 18 U.S.C. 2703(h).

In addition, the CLOUD Act assumes that conflicts of individual laws will be coordinated through the execution of an executive agreement, as detailed in **VI** below.

The proposal for an e-evidence regulation also contains a system that will allow for the filing of an objection to the order for the production of data based on conflicts with applicable laws or regulations of a third country. Where the addressee of the order for production believes that compliance with the order will cause a conflict with applicable laws or regulations of a third country, (s)he may file an objection with the issuing authority and the law enforcement authorities, and the issuing authority will reconsider whether to maintain the order for production. If, as a result of the deliberation, the issuing authority decides to maintain the order, it must ask a court with jurisdiction in the member state for a review, and ultimately follow the decision of that court. In this situation, execution of the order for production will be suspended until the member state court concludes its review.[167]

2. Obtaining Consent of Foreign State Where Server Is Located and Alternative Methods

In situations where data stored in a foreign country is obtained with the consent of the country where the relevant server is located, there are no issues regarding conflicts between national jurisdictions. Therefore, efforts are under way to construct an international framework for obtaining the consent of the country where the relevant server is located. At the same time, an international framework for methods to lawfully exercise enforcement jurisdiction without the consent of the country where the relevant server is located is also being considered.

(1) Mutual Legal Assistance Treaties ("MLATs")

One method by which investigating authorities can investigate a suspect or evidence located in a foreign country is to use diplomatic channels to request mutual legal assistance from the country where the suspect or evidence is located. If the target country has entered into a MLAT with the investigating country, it is also possible for the investigating authorities (*e.g.*, the Ministry of Justice of Japan) to request assistance directly from the relevant authorities in the target country (*e.g.*, the U.S. Department of Justice) without using the above mentioned diplomatic channels.[168]

Although MLAT procedures are easier to carry out than requests through diplomatic channels, in practice, MLAT procedures generally require 6 to 24 months (with an average of 10 months) to complete.[169] Critics state that the time and effort required to use the MLAT procedures prevent expeditious collection of evidence[170] (as a more prompt method, *see* **(2)C.(b)** below for cooperation between the authorities of the signatory countries, as provided by the Second Additional Protocol to the Convention on Cybercrime). Moreover, if the investigative authorities cannot identify the

---

167 Article 16 of EU Electronic Evidence Regulation.

168 For example, see Article 2, paragraphs 2 and 3 of the Treaty between Japan and the United States of America on Mutual Legal Assistance in Criminal Matters.

169 Council of Europe Cybercrime Convention Committee (T-CY) Cloud Evidence Group, *Criminal justice access to data in the cloud: Recommendations*, 9 (2016); Sieber, Ulrich, and Carl-Wendelin Neubert, *Transnational Criminal Investigations in Cyberspace: Challenges to National Sovereignty*, 20 Max Plank Yearbook of United Nations Law 241, 308 (2017); Schwartz, Paul., *Legal Access to The Global Cloud*, 118 COLUM. L. REV. 1681, 1721-1722 (2018).

170 Makoto Ibusuki, *Cross-border Data Flow, Cross-border Search: Legislative Trends in Europe and the US regarding Enforcement Methods Involving Extraterritorial Data Obtainment*, Law & technology, no. 82, p. 47 (2019)

location of the sought-after data and their storage servers at the time of the investigation ("loss of location" of data), MLATs are essentially useless.[171]

(2) The Convention on Cybercrime, the Second Additional Protocol, and the UN Cybercrime Convention

The Convention on Cybercrime is an international convention adopted in 2001 which provides for, among other things, the criminalization of certain acts, such as unauthorized access to a computer system, the establishment of sophisticated criminal procedures relating to expeditious preservation of computer data, international assistance for the extradition of offenders, and other matters.

The Convention on Cybercrime has established certain provisions governing obtaining trans-border data for investigative purposes.[172]

Subsequently, on November 17, 2021, the Committee of Ministers, Council of Europe adopted the Second Additional Protocol to the Convention on Cybercrime, which was signed by 22 states, including Japan, on May 12, 2022. The Additional Protocol will come into force upon ratification by five states, but has yet to come into force. The Second Additional Protocol to the Convention on Cybercrime provides tools for enhanced cooperation and disclosure of electronic evidence, such as direct cooperation with service providers and registrars, effective means to obtain subscriber information and traffic data, and immediate cooperation in emergencies or joint investigations.[173]

On November 18, 2019, the 3rd Committee of the United Nations adopted a draft decision to establish an open-ended ad hoc intergovernmental committee of experts, representative of all regions, (the "**Ad Hoc Committee**") to elaborate on a comprehensive international convention on countering the use of information and communications technologies for criminal purposes,[174] and the decision was adopted by the General Assembly of the United Nations on December 27, 2019.[175] The Ad Hoc Committee was established to discuss the international convention. Then, on May 26, 2021, the General Assembly of the United Nations adopted a decision setting forth the terms for negotiation of the international convention, and after holding six meetings since January 2022, the Ad Hoc Committee decided to submit a draft convention to the 78th session of the General Assembly of the United Nations, to be held in

---

171 UNODC, *Comprehensive Study on Cybercrime*, 217-218(2013), *available at* https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf; Sieber, Ulrich, and Carl-Wendelin Neubert, *Transnational Criminal Investigations in Cyberspace: Challenges to National Sovereignty*, 20 Max Plank Yearbook Of United Nations Law 241, 308 (2017); Schwartz, Paul, Legal Access to The Global Cloud, 118 COLUM. L. REV. 1681, 1721-1722 (2018).

172 Currie, Robert J., *Cross-Border Evidence Gathering in Transnational Criminal Investigation: Is the Microsoft Ireland Case the "Next Frontier"?*, 54 Canadian Yearbook of International Law 63, 77-78 (2017).

173 Council of Europe, *Second Additional Protocol to the Cybercrime Convention on enhanced co-operation and disclosure of electronic evidence (CETS No. 224), available at* https://www.coe.int/en/web/cybercrime/second-additional-protocol.

174 United Nations, *Countering the use of information and communications technologies for criminal purposes : report of the 3rd Committee : General Assembly, 74th session,* A/74/401 (25 Nov. 2019), *available at* https://digitallibrary.un.org/record/3837326?ln=en.

175 United Nations, *Countering the use of information and communications technologies for criminal purposes : resolution / adopted by the General Assembly,* A/RES/74/247, (20 Jan. 2020), *available at* https://digitallibrary.un.org/record/3847855?ln=en.

2024.[176] The Ad Hoc Committee published draft provisions for the preamble, the provisions on international cooperation, preventive measures, technical assistance, including exchanges of information, and the mechanism of implementation of the international convention on countering the use of information and communications technologies for criminal purposes (the "**UN Cybercrime Convention**") in preparation for the meeting held in January 2023.[177]

A. Data Production Orders (Article 18)

With respect to requesting data production from entities or persons located within the territory of the investigating country, Article 18 of the Convention on Cybercrime requires member countries (referred to as a "Party" on the Convention on Cybercrime) to take necessary legislative and other measures to authorize the investigating authorities of the member countries to order:[178]

i. "a person in [the Party's] territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium" (Article 18, paragraph 1, item a), and

ii. "a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control" (Article 18, paragraph 1, item b).

According to a commentary on the Convention on Cybercrime, the term "possession or control" in the above article refers to (i) physical possession of the relevant data in the ordering member country's territory, and (ii) situations in which the data to be produced is outside of the person's physical possession but the person can nonetheless freely control production of the data from within the ordering member country's territory.[179] However, with regard to (ii), a dispute exists as to whether the provision includes situations where the targeted data is stored in a foreign country. Specifically, it is disputed whether the Convention on Cybercrime also took into consideration situations where the targeted computer data is stored in a foreign country and whether it is possible to interpret the member countries as having agreed that a member country's investigating authorities may issue an order for

---

176 United Nations, *Countering the use of information and communications technologies for criminal purposes : resolution / adopted by the General Assembly,* A/RES/75/282, (1 June 2021), *available at* https://digitallibrary.un.org/record/3928637?ln=en.

177 United Nations, *Consolidated negotiating document on the preamble, the provisions on international cooperation, preventive measures, technical assistance and the mechanism of implementation and the final provisions of a comprehensive international convention on countering the use of information and communications technologies for criminal purposes,* A/AC.291/19, (19 December 2022), *available at* https://www.unodc.org/documents/Cybercrime/AdHocCommittee/5th_session/Documents/2228246E_Advance_Copy.pdf.

178 The term "subscriber information" as used in Article 18, paragraph 1, item b of the Convention of Cybercrime, means "any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data" (Article 18, paragraph 3 of the same convention).

179 Committee of Ministers of the Council of Europe, *Explanatory Report to the Convention on Cybercrime*, 29 (2001), *available at* https://rm.coe.int/16800cce5b

submission of data to a person located in the Party's territory or a service provider providing services in the member country's territory in such situations.[180]

Further deliberations are likely to continue in order to set up criteria for the exercise of jurisdiction in situations where the location of data storage is unclear.

B. Trans-border Access to Data (Article 32, item (b))

Article 32, item (b) of the Convention on Cybercrime permits access to data stored on a server located in a foreign country "if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party," namely, if consent is obtained from the Data Subjects (including the relevant service providers, if the server-managing entities have the contractual authority to disclose the stored data).[181]

With respect to the relationship between the act mentioned in item (b) of this article and national sovereignty or enforcement jurisdiction, this provision could be seen as an exceptional provision which authorizes the exercise of jurisdiction within the territory of a foreign country; there is also a view that the act mentioned in item (b) of this article does not fall within the category of an act that "interferes" in the jurisdictional matters of the country where the server is located.[182]

In addition, the drafters of the Convention did not consider item (b) of Article 32 to prohibit or preclude investigations beyond this article, namely, investigations without the consent of the Data Subject. Therefore, additional solutions may be agreed upon at a later stage.[183] Although this point

---

180 In this respect, the U.S. Deputy Assistant Attorney General explains that the CLOUD Act has been enacted as fulfillment of the country's duty under Article 18, paragraph 1, item a of the Convention on Cybercrime (*Deputy Assistant Attorney General Richard W. Downing Delivers Remarks at the Academy of European Law Conference on "Prospects for Transatlantic Cooperation on the Transfer of Electronic Evidence to Promote Public Safety"*, April 5, 2019, available at https://www.justice.gov/opa/speech/deputy-assistant-attorney-general-richard-w-downing-delivers-remarks-academy-european-law); Toshihiro Kawaide, *Computer Network and Cross-border Investigations* in *Commemorative Collection for the 70th Anniversary of the Birth of Professor Masahito Inoue*, pp. 414 and 416, footnote 6 (Yuhikaku Publishing, 2019).

181 Examples of situations under item (b) of Article 32 of the Convention of Cybercrime include: (i) where a legally authorized Data Subject obtains e-mail data stored by an SPC on a server located in a foreign country or intentionally stored by that Data Subject on a server located in a foreign country, and voluntarily submits the relevant e-mail to an investigating authority; or (ii) where a mail box is placed in the personal computer or mobile phone of an arrested suspect, and if the suspect voluntarily consents that the investigating authority access the account and if the investigating authority are sure that the data of the mailbox is located with another member country, the investigating authority may access the data (Council of Europe Cybercrime Convention Committee (T-CY)), *T-CY Guidance Note # 3: Transborder Access to Data (Art. 32)* (op. cit. n. 70), 4-5 (2014) *available at* https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726a).

182 UNODC, *Comprehensive Study on Cybercrime*, 218 (2013), *available at* https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf, Council of Europe Cybercrime Convention Committee (T-CY), *Transborder access and jurisdiction: What are the options?*, Doc No T-CY (2012)3 , 27 (2017).

183 Council of Europe Cybercrime Convention Committee (T-CY), *Transborder access and jurisdiction: What are the options?*, Doc No T-CY (2012)3 , 27 (2012) *available at* https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e79e8.

was not negotiated due to a lack of time to reach an agreement within the timeframe for deliberation of the Second Additional Protocol,[184] deliberations are ongoing.[185]

C. The Second Additional Protocol

The Second Additional Protocol to the Convention on Cybercrime has significance in that it establishes procedures to enhance cooperation with persons located in other signatory countries and authorities of other signatory countries, and establishes provisions concerning protection of personal information.

(a) Direct cooperation with persons located in other signatory countries

Article 6 of the Second Additional Protocol to the Convention on Cybercrime provides for demands to disclose domain name registration information held or managed by the domain registrar located in other signatory countries, and Article 7 provides for orders to disclose subscriber information held or managed by service providers located in other signatory countries. The former provision was established because many cybercrimes involved criminals creating and using internet domains for malicious, unjust purposes (such as disseminating malware or fraud), and access to information concerning who registered the domain was considered extremely important in order to identify the suspects.[186] The latter provision was established because subscriber information is basic information necessary for investigation of cybercrimes and other crimes that require electronic evidence, and the degree of infringement of privacy inherent in its disclosure is lower than that created by disclosure of other types of data.[187]

Articles 6 and 7 of the Second Additional Protocol to the Convention on Cybercrime are structured in fundamentally the same manner; paragraph 1 states that signatory countries are required to adopt legislative and other measures that are necessary to grant the competent authorities within their countries the power to demand or issue an order to disclose information held or managed by a person located in another signatory country. In paragraph 2, they state that signatory countries are required to adopt legislative and other measures that are necessary for allowing persons within in their territory to disclose information pursuant to a demand or order from another signatory country. However, while Article 6 merely grants the competent authorities within their countries the power to "demand" that the domain registrar located in the territory of another signatory country produce domain name registration information, Article 7 not only grants the competent authorities within their countries the power to directly "order" that service providers located in the territory of another signatory country disclose subscriber information, but also allows them to reserve the right not to apply Article 7 in their

---

184 Council of Europe, *Explanatory Report to the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence*, paragraph 24 p. 5 (2022), *available at* https://rm.coe.int/1680a49c9d.

185 Council of Europe Cybercrime Convention Committee (T-CY), *Report on the 27th Plenary of the Cybercrime Convention Committee Strasbourg and online, 29-30 November 2022*, Doc No T-CY (2022)23, p. 4 (2022), *available at* https://rm.coe.int/t-cy-2022-23-plen27-rep-v5/1680a93b1c.

186 Council of Europe, *Explanatory Report to the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence*, paragraph 74 p. 13 (2022), *available at* https://rm.coe.int/1680a49c9d.

187 Council of Europe, *Explanatory Report to the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence*, paragraph 92 p. 17 (2022), *available at* https://rm.coe.int/1680a49c9d.

countries (paragraph 9 of the same article).[188] While signatory countries that reserve their rights for Article 7 not to apply in their countries do not need to take measures pursuant to paragraph 2 of that article for service providers located in their territories to disclose subscriber information pursuant to an order issued by another signatory country, due to the principle of reciprocity, they are not allowed to issue an order to a service provider located in another signatory country seeking disclosure of subscriber information pursuant to paragraph 1 of the same article.[189]

As such, if Japan ratifies the Second Additional Protocol to the Convention on Cybercrime and establishes the necessary legislative and other measures, Japan will be able to make a direct demand to a domain registrar located in another signatory country seeking disclosure of domain name registration information, or make a direct order that a service provider located in another signatory country disclose subscriber information (provided that in the case of the latter, only if the other signatory country has not made a reservation against the applicability of Article7)(*see* **IV.1.(3)A**).

(b) Cooperation with Other Signatory Countries' Authorities

Article 8, Paragraph 1 of the Second Additional Protocol to the Convention on Cybercrime allows each signatory country to empower its competent authorities to issue an order to be submitted as part of a request to another signatory country for purposes of compelling a service provider in the requested signatory country's territory to produce stored subscriber information and traffic data in that service provider's possession or control. Each signatory country is required to adopt such legislative and other measures as may be necessary to give effect to an order submitted by a requesting signatory country (Article 8, Paragraph 2).

This procedure allows more expeditious disclosure of subscriber information and traffic data, compared with the procedures available through MLATs (*see* **(1)** above). The requesting signatory country shall submit the order, the supporting information, and any special procedural instructions to the requested signatory country (Article 8, Paragraphs 3 and 4), and the requested signatory country shall make reasonable efforts to serve the service provider with the order within forty-five days from the date of receipt of all of the information. The requested signatory country shall order the service provider to return the requested information or data no later than twenty days for subscriber information, and forty-five days for traffic data (Article 8, Paragraph 6a).

Although each signatory country is allowed to reserve the right not to apply Article 8 to traffic data (Article 8, Paragraph 13), if Japan ratifies the Second Additional Protocol to the Convention on Cybercrime and establishes the necessary legislative and other measures, Japan will be able to request that a service provider located in another signatory country submit subscriber information and traffic data through the signatory country (with regard to traffic data, only if the requested signatory country has not made a reservation against applicability of Article 8). A signatory country that reserves the right not to apply Article 8 to traffic data in the country will not be required to respond to orders to submit traffic data issued by other signatory countries to service providers located in the signatory

---

188 The relationship with domestic laws is also important in considering whether to reserve the right not to apply part of the Second Additional Protocol to the Convention on Cybercrime in their countries (*see* **VI.2.(2)** below for the relationship with a foreign government's demand or order to disclose information and the Telecommunications Act and Personal Information Protection Act).

189 Council of Europe Cybercrime Convention Committee (T-CY), *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence: Explanatory Report,* paragraph 122 (17 November 2021) *available at* https://search.coe.int/cm/pages/result_details.aspx?objectid=0900001680a48e4b#globalcontainer.

country's territory, but pursuant to the principle of reciprocity, cannot issue orders to submit traffic data to service providers located in other signatory countries based on Paragraph 1 of Article 8.[190]

(c) Provisions on Protection of Personal Information

Article 14 of the Second Additional Protocol to the Convention on Cybercrime provides for detailed obligations relating to measures to protect personal information.[191]

For example, Paragraph 4 of Article 14 lists the following as "sensitive data": personal data that reveals racial or ethnic origin, political opinions, religious or other beliefs, or trade union membership, genetic data, biometric data considered sensitive in view of the risks involved, or personal data concerning health or sexual life, and provides that processing of such data by a signatory country shall take place only pursuant to appropriate safeguards, to guard against the risk of unwarranted prejudicial impact arising from the use of such data, and in particular against unlawful discrimination.

Furthermore, Paragraph 11 of Article 14 imposes on each signatory country the obligation to provide notice, through the publication of general notices, or through personal notice to the individuals whose personal data have been collected, with regard to: (i) the legal basis for and the purpose(s) of processing; (ii) any retention or review periods; (iii) recipients or categories of recipients to whom such data are disclosed; and (iv) access, rectification and redress available. Thus, as with the proposed EU electronic evidence regulation, systems have been introduced to ensure a certain degree of transparency to Data Subjects whose information is disclosed. In this respect, we believe that it is necessary to consider establishing a system for notice to Data Subjects in Japan based on the balance between protection of due process of law for Data Subjects and ensuring the effectiveness of investigations (*see* **IV.1.(3)B.(a)** above).

D. Draft of the UN Cybercrime Convention

The draft UN Cybercrime Convention, published on December 19, 2022, includes provisions similar to those in the Convention on Cybercrime and the Second Additional Protocol to the Convention on Cybercrime.

Specifically, discussions are in progress in granting signatory countries the authority to engage in the following two acts, as part of mutual legal assistance:

(i) requesting that another signatory country order or otherwise obtain the expeditious preservation of [data] [information] stored by means of a [computer system] [information and communications technology system/device] located within the territory of the other signatory country and in respect of which the requesting signatory country intends to submit a request for mutual assistance in the search or similar access to, seizure or similar securing of, or disclosure of the [data] [information] (Article 68, Paragraph 1); and

---

190 Council of Europe Cybercrime Convention Committee (T-CY), *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence: Explanatory Report,* paragraph 147 (17 November 2021) *available at* https://search.coe.int/cm/pages/result_details.aspx?objectid=0900001680a48e4b#globalcontainer.

191 However, if both the transferring country and the receiving country are mutually bound by an international agreement that establishes a comprehensive framework between those signatory countries for the protection of personal data, which meets certain requirements, the terms of that agreement shall apply instead of the provisions of the article (Paragraph 1.b of the article). If there is no international agreement as described above, the transferring country and the receiving country may mutually determine that the transfer of personal data may take place on the basis of other agreements or arrangements (c of the paragraph).

(ii) requesting that another signatory country search or similarly access, seize or similarly secure, and disclose [data] [information] stored by means of a [computer system] [information and communications technology system/device] located within the territory of the requested signatory country including [data that have] [information that has] been preserved pursuant to Article 68 (Article 70, Paragraph 1).

Article 72 provides for cross-border access, and granting signatory countries the authority to engage in the following two acts (subject to a reservation) without the authorization of another signatory country is being considered:

(i) access publicly available (open source) stored [computer data] [electronic/digital information], regardless of where the [data are] [information is] located geographically; and

(ii) access or receive, through [a computer system] [an information and communications technology system/device] in its territory, stored [computer data] [electronic/digital information] located in another signatory country, if the signatory country accessing or receiving the [data] [information] obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the [data] [information] to that signatory country through that computer system.

The proposal for the UN Cybercrime Convention is planned to be submitted at the 78th session of the United Nations General Assembly, to be held in 2024. However, considering that discussions based on a draft commenced in January 2023, unless the negotiations are accelerated, it is highly likely that it will take some time to sign the UN Cybercrime Convention. It is important to pay close attention to future progress in the negotiations, because discussions on mutual legal assistance and cross-border access in connection with cybercrimes also are taking place at the United Nations.

(3) Executive Agreement

Executive agreements under the CLOUD Act have the function of clarifying that a disclosure order issued to a company which is subject to the jurisdiction of one country will not infringe the sovereignty of the other country, at least as between two countries that have entered into an executive agreement, because consent is obtained from the other country.

For example, under the executive agreement between the U.S. and the U.K., either country (the "**Issuing Country**") is able to make a direct request that a service provider in the other country submit data pertaining to serious criminal offences (criminal offences punishable by a custodial sentence of at least three years) under the law of the Issuing Country (Articles 1, 4, and 5 of the agreement).

Specifically, the Issuing Country may issue disclosure orders for data in compliance with its domestic law, subject to review or oversight by a court or other independent authority (these orders may not be issued at the request of the other country or a third-party country) (Article 5, Paragraphs 1 through 4). The Issuing Country may issue orders directly to a provider in the other county through its designated authority (governmental entity designated, for the United Kingdom, by the Secretary of State for the Home Department, and for the United States, by the Attorney General) (without involving the other country's authorities) after reviewing the orders for compliance with the executive agreement (Article 5, Paragraphs 5 and 6). Each order must include a written certification that the order complies with the domestic law of the Issuing Country and the executive agreement, and the Issuing Country must notify the relevant provider that it is invoking the executive agreement with respect to the order, and must provide a point of contact at the designated authority (Article 5, Paragraphs 7 through 9). In response thereto, providers may provide data directly to the Issuing Country's designated authority (Article 6, Paragraph 1). However, the U.K. has the right under the executive agreement to deny the use of the relevant data at trial in a case in which the death penalty is sought in the U.S., and the U.S. has the same right in a case in the U.K. that raises free speech concerns (Article 8, Paragraph 4).

The executive agreement between the U.S. and Australia contains similar provisions to those in the executive agreement between the U.S. and the U.K. While the executive agreement between the U.S. and Australia provides that the issuing country's requirements concerning the manner in which a provider responds to an order may include the requirement that the order and any information or evidence furnished in response be kept confidential (Article 6, Paragraph 4 of the executive agreement between the U.S. and Australia), the executive agreement between the U.S. and the U.K. does not expressly contain such a provision. However, considering that the agreement does provide that the issuing country's investigating authorities may make arrangements with providers for the secure transmission of data produced in response to orders, it is likely that similar treatment to that afforded under the executive agreement between the U.S. and Australia may apply.

VI. Issues Regarding the Execution of an Executive Agreement under the CLOUD Act

1. Functions of an Executive Agreement

As stated in **III.1(2)** above, the functioning of the CLOUD Act depends upon the U.S. government and a foreign government entering into executive agreements, and those executive agreements are expected to set forth the proper form of data disclosure orders directly issued to a provider, as well as how to comply with those orders. One function of these executive agreements is to clarify that a disclosure order issued to a company over which the issuing country has personal jurisdiction does not infringe on the sovereignty of the other country, at least, as between the two signatories to the executive agreement. In addition, an executive agreement should eliminate potential conflicts of law between the signatory country and the U.S. (*see* **V.1.(3)**).[192] If it becomes possible to digitize requests, issuance, and execution of warrants, and if a system for Orders to Produce Electromagnetic Records in electronic form is also introduced in Japan, the institutional groundwork will be laid for maximizing the effect of Japan's collaboration with investigating authorities in foreign countries, such as the U.S., which already have digitized criminal procedures, and carry out investigative activities where data itself is the subject.

Below, we first will highlight specific issues under Japanese law that may arise in situations where Japan enters into an executive agreement with the U.S. and the U.S. government orders a Japanese business operator to submit data under the CLOUD Act.[193] Then, with these issues in mind, we will discuss the points that should be considered when designing such an executive agreement.

2. Relationship Between Japanese Domestic Laws and Investigative Activities Pursuant to the CLOUD Act

(1) Relationship with the Constitution of Japan

Under the CLOUD Act, a Japanese company over which the U.S. government has jurisdiction could be requested by the U.S. government to disclose data pursuant to a warrant or other legal process.

The Constitution of Japan does not apply to acts of an investigating authority of a foreign country. Therefore, if a Japanese company is requested by the U.S. government to disclose data pursuant to a warrant or other legal process, there will be no immediate conflict with the Constitution of Japan.

However, because the process under the CLOUD Act regarding the above-mentioned warrant (or other legal process) does not include the issuance of a warrant by a Japanese court (Article 35 of the Constitution), it is necessary to consider whether or not allowing data to be disclosed to the U.S. government upon its request conflicts with a duty to protect Japanese people's constitutional rights, which may be owed by the government of Japan, or, in order to fulfill that duty, whether or not it is necessary to ensure, through an executive agreement or other appropriate mechanisms, that a request

---

192 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*, 4-5 (2019), *available at* https://www.justice.gov/opa/press-release/file/1153446/download.

193 Separate consideration is required to highlight the issues that may arise under U.S. law in situations where the Japanese government orders a business operator in the U.S. to submit data pursuant to Japanese law.

from the U.S. government under the CLOUD Act satisfies the due process requirements under the Constitution of Japan (Article 31).[194]

(2) Relationships with Other Laws and Regulations

A. Telecommunications Business Act

Under the Telecommunications Business Act, when a telecommunications carrier in Japan is ordered by the U.S. government to disclose data containing information protected under the "secrecy of communications," obeying that order may infringe upon the "secrecy of communications" and therefore constitute a criminal infringement of the secrecy of those communications (Articles 4 and 179 of the Telecommunications Business Act). In this respect, it is necessary to consider, for example, whether or not the disclosure may be deemed to be based on valid consent from the data subject to which the secrecy of communications relates, or otherwise legally justified in some way, such as by qualifying as an Act Performed in Accordance with Laws and Regulations (Article 35 of the Penal Code) or as an aversion of present danger (Article 37 of the Penal Code), and would therefore be permissible under the Telecommunications Business Act.

Since only an act performed in accordance with Japanese laws and regulations is considered to be qualified as an Act Performed in Accordance with Laws and Regulations,[195] compliance with a foreign warrant could not be justified as an Act Performed in Accordance with Laws and Regulations.

On the other hand, the scope of legal interests that can be legitimately protected as an aversion of present danger under the Penal Code is thought, in some cases, to include legal interests in the life and body of each individual, including those without Japanese nationality and located in a foreign

---

194 Similarly, the requirements of due process must be satisfied if Japan and the U.S. hypothetically enter into an executive agreement, and Japanese investigating authorities are directly requiring a U.S. company to submit data based on Japanese law.
Because international assistance in investigations is based on the assumption that the requirements and procedures for the act of obtaining evidence may differ on a country-by-country basis, the extent that the use of evidence obtained via international assistance in investigations constitutes a breach of due process in Japan has been considered comparatively limited compared with cases in which evidence is directly obtained by Japanese investigating authorities. (Toshihiro Kawaide, *Admissibility of Evidence Obtained by International Legal Assistance*, Kenshuu, no. 618, pp. 3, 7 (1999); Supreme Court, Decision dated October 31, 2000, *Keishu* vol. 54, no. 8, p. 735, et. al). By contrast, the admissibility of data that Japanese investigating authorities obtain directly from a U.S. company based on the executive agreement might be evaluated in accordance with the framework for evaluation of the admissibility of data directly obtained by Japanese investigating authorities in Japan, and not the framework for evaluation of the admissibility of data obtained via a request made to U.S. investigating authorities through international assistance in investigations. Given this, it may be possible to say that entering into an executive agreement has the effect of clarifying that assurance of due process, including evaluation of evidence pursuant to the Constitution of Japan and the Code of Criminal Procedure Act of Japan, extends to the acquisition of data located overseas by Japanese investigating authorities.

195 *See* Hidenaga Miyamoto, *Paradigms of Criminal Law*, p. 227 (Kobundo, 1931); Criminal Law Theory Study Group, *Fundamental Principles of Modern Criminal Law (General Theories)*, 3rd ed.], p. 228 (Sanseido, 1996).

country.[196] In light of this, if the government of a foreign country issues a disclosure order in connection with a criminal offense involving an individual located in a foreign country, then there is possibly room to find that compliance with such would constitute an aversion of present danger. To determine the scope of a valid finding that a disclosure was an aversion of present danger, we should consider the elements required for such a finding, such as the substance and degree of the respective legal interests protected under the secrecy of communication, whether or not there is an alternative which could suffice instead of the disclosure, and the balance of the relevant legal interests. Consideration should also be given to making the effects of the executive agreement foreseeable to the responding telecommunications business operators.

With respect to the regulations for specified user information under the Amended Telecommunications Business Act (*see* **IV.1.(3)E(a)** above), matters to note in relation to the U.S. government's investigative activities based on the CLOUD Act are those pertaining to reports of leakages of specified user information. Under the Amended Telecommunications Business Act, Designated Telecommunications Carriers are required to make reports to the Minister of Internal Affairs and Communications when certain specified user information is leaked,[197] and the relevant specified user information includes "information provided to a foreign government pursuant to a legal system in a foreign country that might have an effect on the appropriate handling of specified user information."[198]

The draft amendment to the Commentary on Guidelines for the Amended Telecommunications Business Act states that "a legal system in a foreign country that might have an effect on the appropriate handling of specified user information" refers to a system under which a government may collect specified user information held by Designated Telecommunications Carriers by imposing an

---

196 With respect to the existence or absence of a "present danger," as one of the required elements of an aversion of present danger, some courts have suggested that the existence of a "present danger" may be found even if the danger to the life or body of an individual is to that of an individual who is not a Japanese national and is located in a foreign country: Fukuoka High Court, Judgement, September 17, 1965, *Kakeishu* [Lower Court Criminal Case Report], vol. 7, no. 9, p. 1778; and Matsue District Court, Judgment, July 22, 1998, *Hanrei-jiho*, no. 1653, p. 156 (However, the appellate court (Hiroshima High Court (Matsue Branch), Judgment, October 17, 2001, *Hanrei-jiho*, no. 1766, p. 152) refused to find an aversion of present danger without addressing whether or not a present danger existed) (Noriyuki Nishida et al. (ed.), *Commentary on Penal Code, Vol. 1: General Theories*, §§1-72, p. 480 (Yuhikaku Publishing, 2010) [the part written by Shinya Fukamachi]). With respect to the blocking of information which violates the prohibition against child pornography, there is a view that even if the server on which the relevant child pornography is stored is located overseas, and even if the person with management authority over the server is located overseas or their location is unknown, then irrespective of whether the children victimized by the relevant pornography are Japanese or foreign nationals, an act of blocking the child pornography in Japan is an aversion of present danger and therefore it is not illegal. *See* Japan Internet Safety Promotion Association, Child Pornography Working Group, Report by Sub-working to Consider Legal Issues, p. 18 (publicized on March 30, 2010) (https://www.good-net.jp/investigation/working-group/anti-child-porn_category_112/2010_169-1751_475).

197 Article 28, paragraph 1, item 2(b) of the Amended Telecommunications Business Act.

198 Article 58, paragraph 1, item 2 of the Amended Enforcement Regulation of the Telecommunications Business Act.
Article 18, paragraph 1, item 1 of the Enforcement Regulations of the Act on the Protection of Personal Information, which provide measures that are necessary to ensure continuous implementation of appropriate measures by a third party in a foreign country, is said to have been referenced in formulating the language " a legal system in a foreign country that might have an effect on the appropriate handling of specified user information" (the Ministry of Internal Affairs and Communications, *Opinions on Draft Ministerial Ordinance for Partial Revisions to Regulations for Enforcement of the Telecommunications Business Act and View Concerning the Foregoing* (Matters other than matters that require consultations with the committee)" (https://public-comment.e-gov.go.jp/servlet/PcmFileDownload?seqNo=0000246510), p. 17).

obligation on the relevant Designated Telecommunications Carrier to cooperate with the government's information collection activities, and is limited to systems that may have a material impact on the rights and interests of users with respect to the specified user information,[199] and that disclosure of specified user information pursuant to such a system is subject to leakage reports.[200] In the future, in practice, it will be necessary to pay close attention to whether having to make a leakage report for data disclosure in accordance with the U.S. legal system will cause any hindrance to investigative activities in the U.S.

B. Act on the Protection of Personal Information

Under the Act on the Protection of Personal Information, business operators who handle personal information are in general prohibited from disclosing that personal data of a Data Subject to third parties (located in a foreign country) without the consent of the Data Subject (Article 27, paragraph (1) and Article 28 of the Act on the Personal Information). The act provides certain exceptions to this which allow for the lawful disclosure of information to third parties, including cases where the disclosure is in accordance with laws and regulations (item (i) of the same paragraph). However, the Japanese government appears to understand that the term "laws and regulations" in this article does not include foreign laws or regulations.[201] The act also recognizes that with regard to disclosures made in cooperation with the national government or another government's performance of functions which have been established by laws and regulations (item (iv) of the same paragraph), it is understood that the term "laws and regulations" does not include foreign laws or regulations and that the reference to national governments or other governments does not include those of foreign countries. Therefore, because none of the exceptions apply, if the U.S. government orders a business operator in Japan who handles personal information to disclose personal information, obeying the order without obtaining the consent of the Data Subject is likely to violate the Act on Protection of Personal Information. In addition, even if a business operator intends to obtain the consent of the Data Subject, it may be necessary to consider the extent to which, and how, information based on "other systems that may have a significant impact on the rights and interests of the individual,"[202] as published by the Personal Information Protection Commission, should be provided.

---

199 *Old/new Comparison Table of the Partial Amendment to the Commentary on Personal Information Protection Guidelines for Telecommunications Businesses* (*Public Notice of the Personal Information Protection Commission and the Ministry of Internal Affairs and Communications No. 4 of 2022*) (https://www.soumu.go.jp/main_content/000870399.pdf), pp. 78, 51.

200 Ministry of Internal Affairs and Communications, *Solicitation for Opinions on the Draft Amendment to the Personal Information Protection Guidelines for Telecommunications Businesses and its Commentary*, (https://www.soumu.go.jp/menu_news/s-news/01kiban18_01000188.html).

201 Written Answer to Questions about the U.S. CLOUD Act and Measures under the Act on the Protection of Personal Information submitted by a Member of the House of Representatives, Mr. Koichi Matsudaira (Answer No. 227 received on June 25, 2019) (http://www.shugiin.go.jp/Internet/itdb_shitsumon_pdf_t.nsf/html/shitsumon/pdfT/b198227.pdf/$File/b198227.pdf)

202 Personal Information Protection Commission, *Foreign System (U.S.)*, (https://www.ppc.go.jp/enforcement/infoprovision/laws/offshore_report_america/#law)(last accessed on April 14, 2023).

3. Points to Note in Designing an Executive Agreement

In Japan, given Ohira's Three Principles,[203] an executive agreement based on the CLOUD Act would be considered a "treaty," the adoption of which requires the approval of the Diet.[204] In addition, if Japan enters into discussions with the U.S. to enter into an executive agreement, it is necessary to consider the following points in designing the executive agreement.[205]

(1) Adjustment of Domestic Laws in Japan and the U.S.

As stated in **2** above, without any adjustment to the domestic laws of Japan, if the U.S. government issues a disclosure order under the CLOUD Act to a Japanese company, there is a legitimate reason to be concerned that compliance with the order would be inconsistent with the Constitution and domestic laws of Japan.

In this respect, under the CLOUD Act, it is considered possible to specify, in the applicable executive agreement, more strict requirements for a disclosure order issued by the counter-party country.[206] For example, in order to obtain a subpoena under U.S. law, only the existence of a reasonable suspicion is required, by contrast with warrants, which require probable cause. The degree of specificity that must be used in describing the subject items for a subpoena is also more lenient than that in an examination for a warrant in Japan. Given these factors, it is advisable to carefully consider the requirements for each evidence-gathering system in the U.S. that could be applied to a Japanese entity and to ensure that such systems employ the same level of requirements as those for an examination for a warrant in Japan. In addition, an executive agreement must clearly establish how to handle each

---

203 Ohira's Three Principles stipulate that the Diet's approval is required under Article 73, item (iii) of the Constitution of Japan with respect to: (i) international agreements that include any matters that must be formally prescribed by law (for example, a situation where the conclusion of the international agreement requires new legislative measures), (ii) international agreements that include any financial matter, and (iii) politically important international agreements. By contrast, in the case of an international agreement that provides for details in regard to implementation of a treaty already approved by the Diet or an international agreement that is permitted to be implemented within the scope of the predetermined law or budget, no Diet approval is required. Thus, no Diet approval is required for an executive arrangement that may be concluded within the scope of the authority to handle diplomatic affairs (item (ii) of the same article) vested in the executive power (Minister of Foreign Affairs Ohira's Answer about Treaties to be Approved by the Diet (February 20, 1974); Soji Yamamoto, *International Law (New Edition)*, pp. 106-109 (Yuhikaku Publishing, 1994).

204 On the other hand, in the U.S., the CLOUD Act provides for Congressional oversight of executive agreements which will operate in conjunction with the CLOUD Act. The act provides that if, within 180 days from the Attorney General's notice of certification of an executive agreement, Congress adopts a resolution disapproving that agreement, then that executive agreement will not come into force (CLOUD Act, Sec.105(a), 18 U.S.C. Sec. 2523(d)).

205 It may become necessary to consider whether or not it is possible to ensure the performance of duties under an executive agreement at the state level in the U.S.

206 For example, the US-UK Executive Agreement acknowledges that a provider's disclosure of data should be consistent with the applicable data protection law of the U.S. and the U.K. (*e.g.* Article 2 of the same agreement). In addition, the same agreement provides that in death penalty cases prosecuted in the U.S. and in cases prosecuted in the U.K. in which freedom of expression may be implicated, when using data obtained under the agreement, the counter-party country's consent must be obtained (Section 8.4 of the same agreement). An academic study including this issue has been published (Madhulika Srikumar et al., *India-US data sharing for law enforcement: Blueprint for reforms* (Jan 17, 2019), *available at* https://www.orfonline.org/research/india-us-data-sharing-for-law-enforcement-blueprint-for-reforms-47425/).

legal protection that exists only in one of the U.S. and Japan and not in the other, such as attorney-client privilege in the U.S.

(2) Clarification of the Terms Used in the CLOUD Act

The CLOUD Act contains ambiguous wording, such as the phrase "intentionally target"[207] and "serious crime."[208] It is important to clarify the meanings of those words so that no investigation process will stagnate due to doubts about the proper interpretation of those words.[209]

(3) Protection of Japanese Nationals

If U.S. citizens are targeted by a foreign government, the CLOUD Act requires that the matter be governed by MLATs, as has previously been the case.[210] Therefore, it is plausible for Japan to invoke MLATs, under the reciprocity principle, if Japanese people are targeted by a U.S. investigation. The US-UK Executive Agreement stipulates that each country will not intentionally target people[211] located in the other (Section 4.3 of the same agreement).

In addition, it is important to put a mechanism in place that ensures appropriate protection of the rights and interests of the Japanese government or Japanese citizens, in preparation for situations where the U.S. government may issue a disclosure order based on the CLOUD Act. For example, it may be meaningful (although ordinarily difficult to envisage) to consider a situation in which U.S. investigating authorities are considering whether to issue an order to disclose the Japanese government's data and data held by the Japanese government in the Government Cloud (i.e. a common cloud environment for the Japanese government agencies that the Digital Agency is taking the initiative to put in place) to a cloud service provider that operates the Government Cloud, in connection with a U.S. criminal investigation, and to deliberate whether to organize a place for direct discussions and adjustments between the U.S. and Japanese investigating authorities as to whether the disclosure order is necessary prior to the issuance of the disclosure order. Furthermore, it seems possible to ensure a mechanism that enables appropriate protection of the Japanese government's rights and interests by ensuring that, even if an order to disclose data is to be issued because it satisfies the relevant requirements in U.S. laws and regulations, the cloud service provider also would be allowed to examine whether the relevant requirements are satisfied, consider whether grounds for modification or revocation of the disclosure order, including international concessions, may exist,

---

207 CLOUD Act Sec.105(a), 18 U.S.C. Sec. 2523(b)(4)(A)

208 CLOUD Act Sec.105(a), 18 U.S.C. Sec. 2523(b)(4)(D)(i)

209 For example, the US-UK Executive Agreement defines the term "serious crime" as a crime subject to long-term imprisonment for three years or more (1.14 of the same agreement).

210 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*, p.12 (Apr. 2019), *available at* https://www.justice.gov/opa/press-release/file/1153446/download.

211 While investigating authorities in the U.K. may not target U.S. citizens, there is no provision to the effect that investigating authorities in the U.S. may not target U.K. nationals or citizens (Article 4, paragraph 3 and Article 1, paragraph 12). It appears that this probably resulted from the U.K. being a part of the EU during negotiations of the US-UK agreement, as EU law prohibits discriminatory treatment of citizens of different Member States (Theodore Christakis, "21 Thoughts and Questions about the UK-US CLOUD Act Agreement", European Law Blog (October 17, 2019)).

make assertions to that effect as necessary, and in some cases, allow the relevant provider to claim sovereign immunity under the U.S.'s Foreign Sovereign Immunities Act.[212]

(4) Impact on Other International Agreements

As a result of the execution of an executive agreement between Japan and the U.S., we can expect that cross-border data acquisition between Japan and the U.S. for investigative purposes will be conducted more smoothly. On the other hand, it is necessary to consider whether or not data transfer in that manner will have any impact on other international agreements and other arrangements entered into by Japan. For example, the EU's adequacy decision regarding Japan under on the EU's GDPR attempts to extend its regulatory arm over international data distribution by imposing regulations on not only cross-border data transfer from EU to Japan, but also cross-border data transfer from Japan to a third country. Thus, it is important that data distribution between Japan and the U.S. should be conducted

---

212 In addition to application guidelines and procurement specifications for the Digital Agency's "Provision of Cloud Services for Government Cloud Development - Solicitation for FY2022- ," *see* answer by government witness Mr. Kusunoki during the meeting of the House of Representatives Committee on Cabinet on March 25, 2022 (minutes available at: https://www.shugiin.go.jp/internet/itdb_kaigiroku.nsf/html/kaigiroku/000220820220325012.htm), and answer by government witness Mr. Ninomiya during the meeting of House of Representatives Committee on Cabinet on November 11, 2022 (minutes available at: https://www.shugiin.go.jp/internet/itdb_kaigiroku.nsf/html/kaigiroku/000221020221111007.htm). As can be observed, the mechanism required in order to protect Japan's rights and interests against requests by U.S. investigating authorities for disclosure of data stored on Government Cloud servers is already reflected in the government cloud procurement specifications published by the Digital Agency and is expected to function effectively as the use of government cloud servers spreads among local governments and other entities. Considering that, as described above, because orders for data disclosure from U.S. investigating authorities issued to service providers for the Government Cloud could become a realistic issue only as a result of deliberations, in addition to investigative necessity, matters such as conformity of the data disclosure order with U.S. laws and regulations, review in light of international courtesy, and possible sovereign immunity, the impact of the CLOUD Act on Japan would have no direct relevance to the discussions concerning the Government Cloud, and should be deliberated from a broad perspective covered in this report.

in a manner that maintains an adequately high level of protection for personal information for the GDPR.[213]

(5) Adjustment of Domestic Laws and Regulations

In addition to the execution of an executive agreement, it would be necessary to adjust Japanese laws and regulations to accommodate the CLOUD Act, including enactment of implementing legislation. For example, it is necessary to enact statutory provisions clarifying that accepting a disclosure order issued by the U.S. government under the CLOUD Act neither illegally violates the obligation to maintain the secrecy of communications under the Telecommunications Business Act nor violates the Act on the Protection of Personal Information. In fact, the U.K.[214] and Australia,[215] which already entered into executive agreements with the U.S., entered into those agreements after revising their domestic laws and making necessary adjustments. Incorporating the results of international adjustments into domestic laws also allows Japan to avoid situations where the contents of regulations become layered, complex, and unclear.

---

213 On January 23, 2019, Japan received an adequacy certification notice from the European Commission to the effect that Japan maintains an adequate level of protection for personal data to allow transfer of personal data. On that occasion, the Japanese government accepted the request of the European Commission to explain that a Japanese governmental instrumentality's access to personal data transferred from within the EU to Japan for criminal investigations or national security will be limited to that which is necessary and reasonable and that such access is subject to supervision by an independent organization. Thereafter, on October 26, 2021, it was publicized that the review of the first adequacy certification to be performed within two years after the foregoing notice would be completed by means of publication of reports by both Japan and the EU. On April 3, 2023, maintenance of adequacy was determined, and a report by the European Commission (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=COM:2023:275:FIN) was published, and on April 4, 2023, both the Personal Information Protection Commission and the European Commission published statements that the review was completed. (Japan determined on March 22, 2023 that it would continue to designate the EU and the U.K. as foreign countries that have personal information protection systems recognized as being at the same level as that of Japan.) At the time, the initial adequacy certification was issued before revision of the Act on the Protection of Personal Information in 2021, which covered public and private organizations in a unified manner, including investigating authorities, and local organizations. The European Commission welcomed the Act on the Protection of Personal Information, which covered public agencies in a unified manner (*see also*, the statement in 2. of the European Commission's report). Further discussion is expected in the future concerning the issues presented in this report, based on the assumption that the handling of personal information by Japanese investigating authorities satisfies the requirements of the GDPR.

214 Crime Overseas Production Orders Act 2019 (COPOA).

215 Telecommunications Legislation Amendment (International Production Orders) Act 2021.

VII. Current Situation and Future Course of Ensuring Transparency in Companies

In order to obtain a deeper understanding from Data Subjects and civil society regarding the acquisition of data held by companies for investigative purposes, it is important that companies and industries also make voluntary efforts to ensure transparency. For example, the OECD Government Access Declaration (*see* **Column (i)** above) identifies an aggregated report concerning requests for government access by the private sector as contributing to ensuring transparency in relation to government access.

In fact, data-possessing companies in Japan and foreign countries have begun to issue transparency reports, which publicize the current status of responses and other details regarding requests received from foreign governmental bodies for disclosure of information possessed by them or for deletion of content they possess or control. At present, the content of these publications varies from company to company. However, some companies publicize the number of requests received by type, the rate of cases in which they actually disclosed information, encryption and other protection techniques used upon information acquired from users, etc. These practices are outlined below.

Company	Summary of Disclosed Items
A	Number of responses to user information disclosure/deletion requests; response rate
B	Breakdown of user information disclosure/deletion requests; number of responses; response rate
C	Number of responses to user information disclosure requests; number of responses at each response degree
D	Breakdown of user information disclosure/deletion requests; number of responses; response rate
E	Breakdown of user information disclosure/deletion requests; number of responses; response rate
F	Breakdown of user information disclosure/deletion requests; number of responses; response rate

On the other hand, in April 2020, the Japan Institute of Law and Information Systems (JILIS) published a guideline stating its opinion of what is necessary for business operators to respond to an inquiry from an investigative agency concerning matters related to an investigation.[216] In addition, some companies have drafted policies concerning measures to be taken when the relevant company receives a request for disclosure of information from Japanese investigating authorities, and have published them separately from the transparency reports, which state disclosure policies such as the following (Companies A to E in the following table do not correspond to those in the table on transparency reports above).

---

216 The taskforce for research on "issues related to inquiries concerning investigation-related matters" of the Japan Institute of Law and Information Systems, *Guidelines for Responding to Inquiries concerning Investigation-related Matters*, (1st edition prepared on April 11, 2020)(https://www.jilis.org/proposal/data/sousa_guideline/sousa_guideline_v1.pdf)
As the basic view of a case where an inquiry concerning such matters was received, it states that the business operator should consider (i) whether the inquiry was made legally at first review, and (ii) whether information provided to the investigating authorities has relevance to the investigation, and make a necessary and appropriate report to the investigating authorities (*see* 4. 1.1).

Company	Summary of Disclosure Policies
A	・ Where based on a warrant ・ Where a disclosure request was received in a situation where avoidance of a present danger was established concerning information that constitutes "secrecy of communications" ・ Where an inquiry concerning investigation-related matters was received concerning information that does not constitute "secrecy of communications" and disclosure would not infringe any legal obligation imposed on the relevant company
B	・ Where based on a warrant ・ Where a disclosure request was received for certain information and the disclosure would be necessary and reasonable
C	・ Where based on a warrant ・ Where a disclosure request was received for a rational reason
D	・ (In principle,) where based on a warrant
E	・ Where based on a warrant ・ Where an inquiry concerning investigation-related matters was received for certain information and there is imminent danger to, and public interest in the protection of life, wellbeing, and property, as well as emergency circumstances

The publicizing of information about responses to governmental bodies' disclosure requests, and policies concerning the responses, is gradually being adopted by Japanese companies. By continuing to promote these efforts and improve their transparency, it seems even more possible to promote the protection of Data Subjects and obtain the understanding of civil society, and cooperate with investigations appropriately. Those efforts may give a sense of security to Data Subjects, namely, users of services provided by those companies. Also, those efforts will improve trust in each company within civil society, and eventually enhance each company's competitiveness, especially in the current social climate in which the awareness of the right to privacy has been increasing. When considering a specific framework for the executive agreement, discussions are also expected to take place regarding the desirable formulation of a transparency report or policies concerning responses to (domestic and overseas) investigating authorities' requests for disclosure of information, that is, how to design a user friendly, easy-to-understand report.

＝＝

Column (iii): Ensuring transparency of government access under the Amended Telecommunications Business Act[217]

The Amended Telecommunications Business Act contains an obligation for Designated Telecommunications Carriers to establish and publish their policies on the handling of "specified user information."[218] Because it is necessary for the policy to state the details, purpose and method of use of specified user information to be obtained, safety management methods, and matters relating to

---

217 From the perspective of widely ensuring transparency about the involvement of government agencies other than those in Japan, it is necessary to note, as a relevant policy trend, discussions among the Ministry of Internal Affairs and Communications concerning how to ensure the transparency of content moderation, a screening system relating to the introduction of Designated Important Facilities under the Economic Security Promotion Act, and stealth marketing regulations under the Act against Unjustifiable Premiums and Misleading Representations.

218 Article 27-5 and 27-8, paragraph 8 of the Amended Telecommunications Business Act; and Article 22-2-23 of the Amended Enforcement Regulation of the Telecommunications Business Act.

publication of the time and details of cases involving leaks of "specified user information"[219] during the past ten years, information concerning specified user information provided to a foreign government pursuant to a legal system in a foreign country may be published as well. In this way, in Japan, legal systems to ensure transparency of the status of foreign governments' access to information of users located in Japan are being put in place (including systems to provide information in order to obtain consent to cross-border transfers of personal data (including Information Related to Personal Information) within the meaning of the Act on the Protection of Personal Information), and the discussions in this report are expected to deepen the discussion on these issues, for example, whether or not the subject of this system includes disclosure requests using an executive agreement pursuant to the CLOUD Act, and whether or not similar systems should be put in place for information other than specified user information.

═══════════════════════════════════════

VIII. Future Prospects

1. Relationship Between Cross-border Data Obtainment for Investigative Purposes and the DFFT

To promote digital economies, the Japanese government is advocating for the data economy initiatives (of Japan, the U.S., and European countries) and the realization of the DFFT. The most recent international trade rules, such as the Comprehensive and Progressive Agreement for the Trans-Pacific Partnership (CPTPP Agreement), the United States-Mexico-Canada Agreement (USMCA = NAFTA 2.0), and the Agreement between Japan and the United States of America concerning Digital Trade (Japan-United States Digital Trade Agreement), embody the core principle of the free cross-border transfer of data.[220] There also are ongoing discussions regarding rules for cross-border data transfers in various fora, such as the WTO Joint Statement Initiative on E-commerce and negotiations to include provisions on the free flow of data in the Japan-EU EPA.[221]

However, as more concerns over the effectiveness of data law enforcement are raised as a result of active cross-border data transfer, (while individual business operators should not be prevented from implementing new services and initiatives that take these concerns into account) it follows instead that policies endorsing data localization will spread, and this in turn risks reversing the current trend toward the promotion of cross-border data transfer. In light of this, it is important to ensure that

---

219 *See* **VI.2.(2)A** for details on the amendment of the Telecommunications Business Act concerning leaks of "specified user information."

220 In addition, the core principle is embodied in the Regional Comprehensive Economic Partnership (RCEP) Agreement. However, the Agreement also gives signatory countries more discretion to take measures to restrict cross-border data transfers than CPTPP, and other regulations, and the regulatory level is lower than that of agreements listed in the main text. Furthermore, although the details are yet to be clarified, the Indo-Pacific Economic Framework for Prosperity (IPEF), which is currently under discussion for rulemaking purposes, also aims to promote and support reliable and secure cross-border data flow in an effort to advance digital trade (*MINISTERIAL TEXT FOR TRADE PILLAR OF THE INDO-PACIFIC ECONOMIC FRAMEWORK FOR PROSPERITY Indo-Pacific Economic Framework for Prosperity (IPEF): Part 1 - Trade*, *available at* https://www.mofa.go.jp/files/100391688.pdf).

221 *See*, for example, Junji Nakagawa & Kazumochi Kometani, *Learning the Strategic Use of International Economic Rules*, pp. 127-142 [Masaaki Komatsu] (2022) for the above trend in formation of digital trade.

investigating authorities can have access to data located in foreign countries to the extent necessary and adequate.[222]

2. Significance of Building an International Framework Among Like-minded Countries

The "Operational Approach" formulated by the Data & Jurisdiction Working Group of I&JPN (*see* **Column (ii)** above) presents (i) the CLOUD Act, (ii) the Proposed EU Electronic Evidence Regulation and Directive, and (iii) the proposed additional protocol to the Convention on Cybercrime, as international frameworks for cross-border data obtainment for investigative purposes, which are expected to become more popular in the future.[223]

The Proposed EU Electronic Evidence Regulation and Directive, via a unilateral legal framework, require that service providers within the scope of its legislative jurisdiction respond to production orders and similar demands, and if the service provider is located outside EU, require that the service provider appoint an agent within EU in order to ensure the effectiveness of the exercise of enforcement jurisdiction. However, there are limitations, such as the inability to exercise enforcement jurisdiction where a service provider located outside EU breaches its obligation and fails to appoint an agent within EU.

On the other hand, if we are able to build up an international framework for obtaining data for investigative purposes among multiple countries, the framework will form a stable foundation for international cooperation in investigations. For this purpose, the Second Additional Protocol to the Convention of Cybercrime, signed in May 2022, should be ratified as soon as possible. However, the Second Additional Protocol only allows a request to disclose domain name registration information to a domain registrar located in other signatory countries and issuance of an order to disclose subscriber information to service providers located in other signatory countries. Beyond this, significant time is expected to be required to reach a multilateral agreement on matters such as issuance of orders to disclose content data to service providers located in other signatory countries.

Therefore, for the time being, it seems effective, from the perspectives of promptness and feasibility, for like-minded countries that share a common sense of values to steadily create bilateral (or multilateral) frameworks, such as the executive agreements envisaged by the CLOUD Act, in

---

222 Kojiro Fujii, *The Data Free Flow with Trust Initiative and Cloud Act: An Overview of Recent EPA Digital Trade Regulations and Introduction to the "Report on Cloud Act",* Nihon Kokusai Keizaiho Gakkai Nenpo, no. 29, p. 56 (2020). The same opinion in: Tomohiro Mikanagi, *The Function of Territorial Sovereignty in International Rules Governing the Use of the Internet*, Kokusai-ho Gaiko Magazine vol. 121, no. 1, pp. 1, 14, footnote 38 (2022).

223 Internet & Jurisdiction Policy Network, *Concrete Proposals for Norms, Criteria and Mechanisms: Operational Approaches* (Apr. 23, 2019), available at https://www.internetjurisdiction.net/news/operational-approaches-documents-with-concrete-proposals-for-norms-criteria-and-mechanisms-released. In addition, as an example of discussion on the establishment of an international framework regarding cross-border transfer of data and restrictions thereon from the perspective of government access, there is Shota Watanabe, *Restrictions on Cross-border Transfer of Data for Reason of Government Access (GA)—Actual Situation, Legal Provisions Under International Trade Law, and Implications for DFFT* (December 2019) (https://www.rieti.go.jp/jp/publications/summary/19120008.html).

accordance with the spirit of the DFFT.[224] As stated in **III.1.(2)** above, these frameworks are being formulated. However, in light of the increasing complexity of cyber crimes, cyber security risks, and geopolitical impact, the progress of building these frameworks, and creation of a framework that is suitably accepted on an international scale is likely to contribute to the construction and practice of Japan's cyber/economic security strategies.

Accordingly, from the perspectives above, it would be worthwhile for Japan to consider the necessary legal issues, with a view to entering into a bilateral (or multilateral) international agreement, as envisaged by the CLOUD Act. Furthermore, when determining which countries should become candidates for execution of bilateral (or multilateral) international agreements, as "like-minded countries" that share a common sense of values, it seems useful to consider this issue from the perspective of whether or not the country shares internationally-accepted principles, such as the OECD Government Access Declaration (*see* **Column (i)** above).

End

---

224 When trying to create a framework among like-minded countries, like an executive agreement under the CLOUD Act, in addition to the Second Additional Protocol to the Convention of Cybercrime, which is a multilateral international framework, it will be necessary to organize the relationship and deliberate as to whether there is any possibility of a conflict arising in situations where both apply, and if so, how to adjust the relationship.

For example, because Article 14 of the Second Additional Protocol to the Convention of Cybercrime sets out detailed obligations concerning personal information protection measures, even if, hypothetically, an executive agreement with a certain country merely provides that personal information will be protected according to the laws and regulations of the country requesting submission (for example, Article 3, paragraph 4 of the US-Australia Executive Agreement), if the relevant country also is a signatory to the Second Additional Protocol to the Convention of Cybercrime, personal information protection measures of the level provided in Article 14 of the Second Additional Protocol must be established with regard to the domain name registration information disclosed by the person located in the relevant country (Article 6 of the Second Additional Protocol) and the registrant information (Article 7 of the same). Accordingly, at least with respect to submission of domain name registration information and registrant information, even if submitted pursuant to the relevant executive agreement, deliberations must take place as to whether it is necessary to put in place relevant domestic laws to ensure that personal information protection measures of the level provided in Article 14 of the Second Additional Protocol to the Convention of Cybercrime apply.

However, if a business operator in a signatory to the Second Additional Protocol discloses data to a non-signatory pursuant to an applicable executive agreement, the foregoing issue will not arise, because the Second Additional Protocol will not apply.