NISHIMURA & ASAHI

Nishimura Institute of Advanced Legal Studies ("NIALS")

Report by the "CLOUD Act Study Group"

— LEGAL ANALYSIS AND PROPOSALS ON CRIMINAL INVESTIGATIONS OBTAINING DATA HELD BY COMPANIES —

[Translation ver. 2 (17 July 2020)]

[This is an English translation of the Japanese original released by NIALS in December 2019.]

December 2019

Nishimura Institute of Advanced Legal Studies

Otemon Tower, 1-1-2 Otemachi, Chiyoda-ku, Tokyo 100-8124, Japan

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>>

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, etc. were supported by the following domestic and overseas communications and IT companies and organizations:

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 represent the views of NIALS and do 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 ····· 4

II. The Study Group's Proposals ····· 4

III. Outline of the CLOUD Act ····· 6

1. Background to Enactment ····· 6
2. Outline of the CLOUD Act ····· 7

IV. Issues Regarding Investigative Authorities' Obtainment and Use of Data Held by Companies Under Japanese Law ····· 9

1. Investigative Means for Obtainment of Data Held by Companies ····· 9
   (1) Analysis of the Current Situation ····· 9
   (2) Collaboration Between Investigative Authorities and Companies ····· 11
   (3) Consideration of a Mid- to Long-Term Systemic Design ····· 13
2. Use of Data Obtained by Investigative Authorities in Criminal Trials ····· 20
3. Issues of Encrypted Data ····· 22
   (1) Relationship with Suspect ····· 22
   (2) Relationship with Third Party Other Than Suspect ····· 23

V. Obtaining Data Stored Overseas for Investigative Purposes ····· 24

1. Without Obtaining Consent of Foreign State, the Situs of the Server ····· 24
   (1) The Concept of Jurisdiction and Issues to be Addressed Regarding International Law ····· 24
   (2) International Law Assessment of Accessing Overseas Data for Investigative Purposes ····· 27
   (3) Coordination of Conflicts Among the Laws of Countries ····· 33
2. Obtaining Consent of Foreign State Where Server is Located and Alternative Methods ·34
   (1) Mutual Legal Assistance Treaties ("MLATs") ····· 35
   (2) The Convention on Cybercrime ····· 35
   (3) US-UK Executive Agreement ····· 39

VI. Issues Regarding the Conclusion of an Executive Agreement under the CLOUD Act ····· 39

1. Functions of an Executive Agreement ····· 39
2. Relationship between Japanese Domestic Laws and Investigative Activities Pursuant to the CLOUD Act ····· 40
   (1) Relationship with the Constitution of Japan ····· 40
   (2) Relationships with Other Laws and Regulations ····· 40
3. Points to Note in Designing an Executive Agreement ····· 42
   (1) Adjustment of Domestic Laws in Japan and the U.S. ····· 42
   (2) Clarification of the Terms used in the CLOUD Act ····· 43
   (3) Protection of Japanese Persons ····· 43
   (4) Impact on Other International Agreements ····· 43
   (5) Adjustment of Domestic Laws and Regulations ····· 44

VII. Current Situation and Future Course of Ensuring Transparency in Companies ····· 44

VIII. Future Prospects ····· 45

1. Relationship Between Cross-border Data Obtainment for Investigative Purposes and the DFFT ····· 45
2. Significance of Building an International Framework among Like-minded Countries ···45

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 investigative authority issues an order to disclose data that a company stores on servers located outside of the US,[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.

NIALS, with Japan's response to the CLOUD Act as a starting point, established the Study Group which seeks to analyze and make proposals 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 inter-state and public-private collaborations. 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 are summarized in this report.

The specific 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. With this in mind, Part **IV** explores the issues relating to criminal investigative methods of 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 measures to obtain data held by companies, including a suggestion for the Japanese government to enter into an executive agreement with the US 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**).

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.

II. The Study Group's Proposals

In recent years, the accumulation of data by 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, a material evidence in the subsequent criminal investigation, is held by a company on servers located overseas. In order for Japanese investigative 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

---

[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 20 below.

stored on the terminals of suspects, but also to obtain data held by companies in Japan and in foreign countries. The CLOUD Act serves as a useful reference for establishing a mechanism to achieve this.

On the other hand, in situations where data held by companies is to be obtained for investigative purposes, it is also necessary to guarantee the rights of the person 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 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 data. Also, where there is a possibility that 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, NIALS proposes:

1. Further Utilizing Existing Investigative Techniques for Obtaining Data Held by Companies, and, in the Mid-Long term, Considering New Systemic Designs

Although under the domestic laws of Japan a system of obtaining data held by companies for investigative purposes already exists and actual practices of the system are developing, issues still remain. In addressing these concerns in the short-term, it is necessary to ensure that investigative authorities obtain data held by companies efficiently and effectively: this can be done by actively utilizing the seizure by an order to produce a copy of records through cooperation with companies, while taking into account the interests of Data Subjects and companies. In the mid- to long-term, it is necessary to advance discussions on the systemic design, from various viewpoints, such as ensuring the fairness and transparency of procedures including the system of notification to Data Subjects and companies, expansion of the system to impose confidentiality obligations and similar restrictions, digitization of warrant proceedings, and to analyze relationships with other laws and regulations concerning data protection (**IV.1** below). In addition, the prospect of the data so obtained being used in a criminal trial should be considered. In other words, 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 From the Perspectives of International Law and Establishing a Cross-national Framework

There are ongoing domestic and international discussions regarding the legality of obtaining data stored outside the territory of an investigative 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 may be argued that obtaining data stored in servers located in the territory of another state for investigative purposes, for example issuing data production orders against a domestic company in relation to its data stored overseas, is not by the method employed necessarily amounts to an unlawful exercise of the investigating country's jurisdiction in the territory of another state. 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).

---

[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 (8) of the Act on the Protection of Personal Information.

Moreover, as for advancing international collaboration, it is not only confined to the development of a multinational framework as represented by the Additional Protocol to the Convention on Cybercrime currently under review, but it can be achieved through regional collaboration as seen in the EU, or collaboration between like-minded countries, as envisioned by bilateral executive agreements under the CLOUD Act. Among these options, it is considered effective for Japan to build a framework with like-minded countries with whom Japan shares a common sense of values in accordance with the trustworthy concept of Data Free Flow with Trust ("**DFFT**"). From this viewpoint, it is desirable to proceed with necessary discussions on legal issues, taking into consideration the execution of bilateral international agreements with like-minded countries, such as the US (**V.2**, **VI**, and **VIII** below).

3. Promoting Companies' Efforts to Ensure Transparency of Public 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 the transparency in the processing of public bodies' requests for data held by companies (public access). These efforts would allow companies to provide a sense of security to users who are Data Subjects and to improve each company's corporate image in civil society, 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 on public access and to make increased efforts in this regard (**VII** below).

III. Outline of the CLOUD Act

1. Background to Enactment

In the U.S., before the enactment of the CLOUD Act, no laws or regulations, including the Stored Communications Act (the "SCA") which provided for procedures to request electronic communication service providers to disclose data, contained provisions that explicitly authorized U.S. governmental bodies to issue an order for the submission of data stored outside of the U.S. On the other hand, 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") but their efficiency and certainty were questioned and the extraterritorial application of the SCA was being debated.

Against this backdrop, when a U.S. investigative 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.[3] and moved to quash the warrant. Although the 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. In this midst of this, voices seeking clarification of the laws and regulations concerning procurement of cross-border data for investigative purposes became louder, which led to the enactment of the CLOUD Act.[4]

---

[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 concluded for the reason that the necessity to make a decision ceased to exist (*U.S. v. Microsoft Corp.*, 138 S. Ct. 1186 (2018)).

2. Outline 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 the U.S. government to compel a provider subject to U.S. jurisdiction[5] to store, back-up, and disclose data held outside of the Unites States 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 concluded an executive agreement (*see* **VI** below).[7] In addition, the provider may also contest the disclosure 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 concluded 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. law.[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 conclude 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 concluded an executive agreement with the U.S. must respond to the U.S. government's orders also.[12]

---

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).

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).

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 the conclusion of 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 the CLOUD Act and conclusion of executive agreements, together, would establish legal provisions of obtainment of data stored in other countries for investigative purposes. In fact, the U.S. government seems to have already commenced negotiations with the so-called Five Eyes[16] and the EU[17] toward conclusion of executive agreements under the CLOUD Act. On October 3, 2019, the U.S. concluded an executive agreement with the United Kingdom (Agreement between the Government of the United States of America and the Government of the United Kingdom of Great Britain and Northern Ireland on Access to Electronic Data for the Purpose of Countering Serious Crime; the "**US-UK Executive Agreement**"),[18] and on October 7, 2019, it publicly announced the commencement of negotiations with Australia.[19]

---

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. 2019), *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.

16 "Five Eyes" refers to the U.S., the U.K., Canada, Australia, and New Zealand.

17 European Commission, *Criminal justice: Joint statement on the launch of EU-U.S. negotiations to facilitate access to electronic evidence* (Sep. 26, 2019), *available at* https://europa.eu/rapid/press-release_STATEMENT-19-5890_en.htm.

18 U.S. Department of Justice, *U.S. And UK Sign Landmark Cross-Border Data Access Agreement to Combat Criminals and Terrorists Online* (Oct. 3 2019), *available at* https://www.justice.gov/opa/pr/us-and-uk-sign-landmark-cross-border-data-access-agreement-combat-criminals-and-terrorists.

19 U.S. Department of Justice, *Joint Statement Announcing United States and Australian Negotiation of a CLOUD Act Agreement by U.S. Attorney General William Barr and Minister for Home Affairs Peter Dutton* (Oct. 7 2019), *available at* https://www.justice.gov/opa/pr/joint-statement-announcing-united-states-and-australian-negotiation-cloud-act-agreement-us.

IV. Issues Regarding Investigative 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[20] by companies. The SCA, as amended by the CLOUD Act, sets out procedures by which investigative authorities can access a large volume of data held by companies. Whereas in Japan, 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, however, due to the subsequent spread of cloud services and for other reasons, the volume of data held by companies is dramatically increasing.[21] 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 Means for Obtainment of Data Held by Companies

(1) Analysis of the Current Situation

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

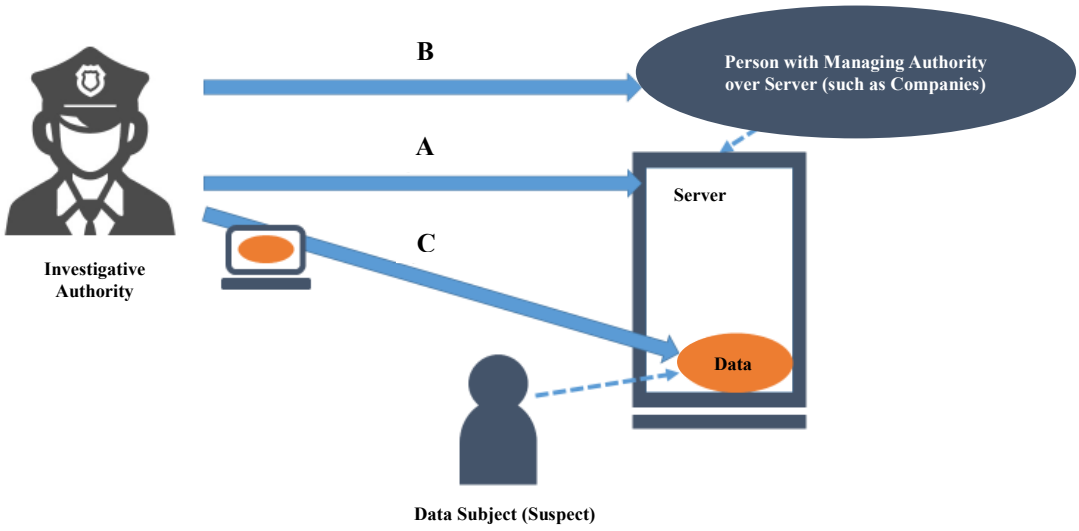

Figure: Classification of means by which an investigative authority obtains data stored on a server managed by a company

---

20 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 managing authority."

21 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 investigative 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 investigative 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 investigative 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 them (*see* **V.1.(2)** below).

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

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

If done by way of compulsory order, the investigative authorities may compel a person with managing 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) of the same code). 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 "electronic or magnetic record to be recorded or printed out" (i.e., data to be disclosed)[22]; therefore, it is not necessary to identify the server on which the targeted data is stored.

As a means that does not constitute a compulsory order, an investigative authority may request a person with managing authority over the relevant server to submit the targeted data using an official inquiry concerning investigation-related matters 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 investigative 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.

The Code of Criminal Procedure has provisions that explicitly authorize this measure and specify the method of copying data from a recording medium (server) connected via telecommunication lines to a computer which is a client terminal and then seize that client terminal ("**Remote Access**") (Article 99, paragraph (2); Article 218, paragraph (2) of the same code). However, with regard to Remote Access, the Code only provides for a measure in which "those electronic or magnetic 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

---

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

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, two approaches have been proposed.[23] The first approach is that after seizing a client terminal, an investigative authority may be able to again request and acquire a seizure warrant that allows it to copy data through Remote Access 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 investigative authority is needing Remote Access, which is ancillary to the seizure.[24]

As a second approach, an investigative 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). However, there is controversy as to 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 pointed out that Remote Access by other means might not be permissible.[25]

(2) Collaboration Between Investigative Authorities and Companies

As stated in **(1)** above, each of the current means of obtaining data held by companies for investigative purposes 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 investigative authorities and companies, as stated in **II** above.[26]

---

23 In addition to the two approaches introduced in the main text, an investigative authority may access the server on which the targeted data is stored as part of a non-compulsory investigation after obtaining consent from the owner of the client terminal. However, as shown by the prohibition on non-compulsory investigation for residences, etc. (Article 108 of the Code of Conduct for Criminal Investigation), even if consent is obtained, this does not mean that there are no issues with regard to the protection of due process of law. There are also court precedents that denied the existence of consent by finding that the person who was subject to the relevant disposition did not give consent based on his/her true intention (Kyoto District Court, Judgment, March 24, 2017, LEX/DB25448598; Osaka High Court, Judgement, September 11, 2018, LEX/DB25449705 (an appeal pending before the Supreme Court)).

24 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)

25 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, which rendered a decision on whether GPS investigation is permissible under an inspection warrant.

26 In an Internet space, in particular, the person with managing 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 managing authority, there is a higher necessity for an investigative authority to obtain information with the relevant company's cooperation when conducting an investigative activity on the Internet (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 Investigative Authorities

According to the interviews conducted by the Study Group with domestic and foreign Internet and technology related companies, many domestic and foreign companies basically cooperate with a seizure by 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 investigation-related matters 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 investigative 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 investigative authorities. This may provide their users with an opportunity to lodge a complaint against the companies regarding their responses to orders or requests from investigative authorities. In addition, some companies release transparency reports in which they clarify the number of disclosure requests that they have received from investigative 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 investigative authorities (*see* **VII** below).

B. Further Utilization of Seizure by Order to Produce A Copy of Records

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

As stated in **(1)C** above, it is difficult to say that Remote Access under the current law is convenient for investigative authorities. On the other hand, as stated in **A** above, many companies actually accept seizures by an order to produce a copy of records. In addition, there are cases where data that has been deleted from a client terminal is still stored on a server managed by a company.[27] Investigative authorities may be able to obtain the data through a person with managing authority over the relevant server by conducting a seizure by an order to produce a copy of records in such cases. In addition, as discussed in **V.1.(2)A** below, a seizure by 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 by an order to produce a copy of records is directed to a company subject to the jurisdiction of Japan. In this regard, a seizure by an order to produce a copy of records can be said to be a more stable means of obtaining data stored on servers.

Additionally, given the current heightened international awareness of privacy protection, it is anticipated that more companies will request a warrant before disclosing data in the future. From this

---

[27] 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.

viewpoint, the means of seizure by an order to produce a copy of records, which is a measure based on a warrant, should be utilized more extensively.[28]

C. Collaboration Between Investigative Authorities and Companies in Connection with the Utilization of Seizure by Order to Produce a Copy of Records

As stated in **(1)B** above, in a warrant of seizure by an order to produce a copy of records, an "electronic or magnetic record to be recorded or printed out" is entered, rather than an "article to be seized."[29] If the "electronic or magnetic 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, investigative 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.

Additionally, in the context of utilizing seizure by an order to produce a copy of records, the specific protocol of presenting a warrant and submitting data can become an issue (for future issues, *see* also **(3)C** below).

Therefore, we expect investigative authorities and companies to seek ways to describe the "electronic or magnetic record to be recorded or printed out" and to utilize seizure by an order to produce a copy of records through their cooperation and in a manner that will facilitate their smooth collaboration.

(3) Consideration of a Mid- to Long-Term Systemic Design

Regarding the measures for obtaining data held by companies, the following issues should be considered from a mid- to long-term perspective.

A 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 procedure to ensure procedural fairness and to protect the rights and interests of the person (Article 222, paragraph (1); and Article 110 of the same code).

---

[28] In the United States, by focusing on an invasion of privacy by the government's acquisition of location information held by wireless carriers in a continuing and comprehensive manner, the Supreme Court 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*, 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.

[29] 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.

However, in situations where an investigative authority obtains data held by a company, a Data Subject who has a material interest in the data is not always subject to the relevant disposition (*see* **(1)** above). Therefore, it is conceivable to consider not only the necessity of presenting a warrant to the person who is subject to the relevant disposition, but also whether additional measures are needed to ensure procedural fairness, such as giving notice to the Data Subject.[30] On this point, the Act on Communication Interception for Criminal Investigation (the "**Communication Interception Act**") 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, the act has a system for giving subsequent notice to the communicating parties (Article 30 of the same act).[31]

Moreover, in cases where investigative authorities use such investigative measures to directly accesses the server on which the targeted data is stored, as represented by Remote Access, the problem of the company not becoming aware of access to the server under its management may arise. In this respect, the German Code of Criminal Procedure authorizes an investigative 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, the person with managing authority over the relevant server must be notified of such disposition.[32]

Quite rightly, as a means of ensuring procedural fairness, in addition to giving notice, there exists a mechanism of having a third party attend the warrant execution (Article 222, paragraph (1); Article 114 of the Code of Criminal Procedure),[33] and it is not always the optimum solution to simply mandate ex post facto notice in all cases where an investigative authority obtains data held by a company. Furthermore, even if a mechanism to give subsequent notice is established, it is necessary to further consider to whom, on what conditions, and at what time the notice should be given.[34] For

---

30 There are instances in which interested individuals may receive notice in the course of certain investigations in Japan. For example, Article 100, paragraph (3) of the Code of Criminal Procedure provides that when postal items are seized, the sender and recipient must be notified. However, where an investigative authority causes a company to record an e-mail and then seizes the e-mail by means of seizure by an order to produce a copy of records, it is understood that the same paragraph does not apply because the sender and recipient can still receive e-mails (Kiyotaka Kunugi, *Pros and Cons of Issuing a Search and Seizure Warrant for E-mails Stored on E-mail Servers of Internet Providers*, Annex Hanrei Times, no. 35, pp. 154 and 155 (2012)).

31 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)

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

33 *See* Supreme Court, Judgment, March 15, 2017, Keishu [*Supreme Court Criminal Case Report*], vol. 71. no. 3, p. 13

34 Subsequent notice under the Communication Interception Act, as mentioned above, is given to the communicating parties named in the interception record, when an interception record (Article 29 of the same act) is prepared. When intercepting a communication, it is permissible to intercept that communication to the minimum extent necessary to determine whether or not it falls within the scope of communications to be intercepted as specified in the interception warrant (Article 14 of the same act). It is not realistic to require notice in all cases of intercepting a communication to decide on the relevancy thereof; rather, there is a risk of causing an invasion of privacy in the course of giving such notice.

example, as pointed out in **B** below, giving notice may cause suppression or concealment of evidence; therefore, the timing of notice should be particularly carefully examined.

When designing the system, it should be borne in mind that there may be cases where a server the targeted data is stored and the company that manages the server are located overseas, and where the server location cannot be identified.

B. Improving System to Impose Duty of Confidentiality on Companies

As stated in **A** above, it is worth considering establishing a system whereby a notice is given to the Data Subject or the person with managing authority over the relevant server when an investigative authority obtains data. Furthermore, as stated in **(2)A** above, some companies have a policy of giving notice to users when they receive an order or request from investigative authorities. However, upon learning an investigation is actually taking place, there may be instances whereby the relevant suspect and other related parties suppress or conceal evidence.[35]

In connection with this, the Code of Criminal Procedure has a system that imposes an obligation of confidentiality on the subject of a warrant (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 by an order to produce a copy of records, is not covered by the confidentiality obligation.[36] 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 investigative authorities. From a mid- to long-term perspective, Japan should consider improving the system to impose a confidentiality obligation on companies. In this respect, it is worth referring to the SCA which authorizes U.S. investigative authorities to seek an order suspending providers' notice in certain cases.[37]

C. Digitization of Warrant Proceedings

It is also important to consider how to strike a balance between judicial control through warrant proceedings and expeditious investigations. In this respect, given the current circumstances where

---

35 As a symbolic example, before the amendment in June 2015 the "Personal Information Protection Guidelines for Telecommunications Businesses" provided, as a requirement for a telecommunications service provider to provide GPS information stored on a user's mobile terminal in response to an investigative authority's request, that the user should be able to know that such location information was obtained through sound or movement of the mobile terminal. However, this requirement was removed in the amendment in June 2015, because it impeded the effectiveness of investigations. For the purpose of the amendment, *see* also "Amendment to the Personal Information Protection Guidelines for Telecommunications Businesses (Draft)" (2015) (https://search.e-gov.go.jp/servlet/PcmFileDownload?seqNo=0000127697), which is material to the public comment procedures regarding the amendment to the commentary on the guidelines.

36 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)

37 18 U.S. Code § 2705(b). There is also an example of legislation that authorizes the U.S. investigative 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)).

efforts to digitize procedures have been made under the so-called "digital procedure act,"[38] Japan should consider speeding up the procedures by promoting computerized or online warrant proceedings.

In fact, in the U.S., online procedures for requesting and issuing a warrant through reliable means are already permitted in many states and at the federal level.[39] On the other hand, in Japan, laws and regulations are based on the premise that a warrant is a physical document (*see* Article 219, paragraph (1) of the Code of Criminal Procedure), and it is provided that a request for a warrant should be filed in writing (Article 139 of the Rules of Criminal Procedure). Therefore, in order to promote digitized or online warrant proceedings, these provisions should be amended, at least, and other legal reforms would also be required.[40] In the process of the interviews conducted by the Study Group with domestic and foreign companies, there were many opinions agreeing that if the digitization of warrant proceedings is achieved, and if the response method also becomes computerized or moves online, it would be easier for companies to cooperate with investigations.

Furthermore, when promoting online procedures, there are issues regarding securing judges who can examine and issue warrants and the impact on decisions on emergency cases where a search is conducted without a warrant.[41] If warrant proceedings actually become digitized, methods for ensuring the security of the online systems would be also an issue.[42] In this respect, a network built by the Securities and Exchange Surveillance Commission named "Compliance WAN"[43] is a useful reference. It is a network using leased lines which serves as a mechanism for market players, including government authorities, to exchange information regarding unfair transactions. Some companies have built an online system for public access and have ensured security by causing investigative authorities to register their e-mail addresses with e-mail domains used by public institutions. In addition, utilizing electronic signature technologies can be a good means to ensure

---

38 The formal name of this act is the "Act Partially Amending Act on Use of Information and Communications Technology in Administrative Procedure and Other Acts for Improving Convenience of Administrative Procedure for Concerned Parties and Enhancing Simplicity and Efficiency of Administrative Operations Through Utilization of Information Communications Technology."

39 In the United States, the trustworthiness of electronic documents and the safety of communications through electronic procedures have increased, and the amount of investigatory materials required for filing a request for a warrant have increased; therefore, an electronic search warrant system was institutionalized in 2006, and arrest warrants, information, and writs of summons were computerized in 2011 (Rule 4.1 of the Federal Rules of Criminal Procedure) (Masatoshi Ishikawa, *Electronic Warrants in the United States*, Sosa-kenkyu, no. 823, pp. 94, 96 (2019), Masatoshi Ishikawa, *Computerization of Warrants and Exclusion of Evidence in the United States*, Aoyama Hogaku Ronshu, vol. 60, no. 4, pp. 99, 102-104 (2019)).

40 The Act on the Use of Information and Communications Technology in Administrative Procedures (the "**Online Administrative Procedures Act**") provides for matters necessary to perform administrative procedures electronically, such as filing an application and issuing a notice of disposition; however, this act does not apply to criminal procedures (*e.g.*, Article 2, item (vi) of the same act).

41 Masatoshi Ishikawa, *Computerization of Warrants and Exclusion of Evidence in the United States*, Aoyama Hogaku Ronshu, vol. 60, no. 4, pp. 111-115 (2019)

42 For discussion of an online system of inquiry concerning investigation-related matters, *see* Comprehensive Security Measures Conference, *Further Promotion of Public-Private Partnership on Cybercrime Investigations and Damage Prevention Measures*, p. 12 (April 2016) (https://www.npa.go.jp/cyber/csmeeting/h27/pdf/h27_honpen.pdf).

43 Securities and Exchange Surveillance Commission, *Commencement of Use of "Compliance WAN"* (January 25, 2009) (https://www.fsa.go.jp/sesc/news/c_2009/2009/20090126.htm)

the authenticity of an electronic warrant (*see, e.g.*, Article 3, paragraph (4) of the Online Administrative Procedures Act).

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

In creating an environment where investigative 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 may apply, in order to make sure that a company disclosing data to an investigative 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).

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 by an order to produce a copy of records is conducted, or cases where any other legal justification is found,[44] 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 15, paragraph (1), item (i) of the Personal Information Protection Guidelines for Telecommunications Businesses,[45] and 3-5-1(1) of the Commentary on these Guidelines).[46]

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 investigation-related matters, which can be conducted without any court order

---

44 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)

45 Ministry of Internal Affairs and Communications, *Personal Information Protection Guidelines for Telecommunications Businesses (Public Notice of the Ministry of Internal Affairs and Communications No. 152 of April 18, 2017)* (September 14, 2017) (http://www.soumu.go.jp/main_content/000507466.pdf)

46 Ministry of Internal Affairs and Communications, *Commentary on the Personal Information Protection Guidelines for Telecommunications Businesses (Public Notice of the Ministry of Internal Affairs and Communications No. 152 of 2017; Latest revision: Public Notice of the Ministry of Internal Affairs and Communications No. 297 of 2017)* (January 2019) (http://www.soumu.go.jp/main_content/000603940.pdf#page=60&zoom=100,0,822)

or warrant.[47] In addition, certain authoritative literature points out that "a very cautious stance is adopted for the secrecy of communications in Japan, and a strict examination of the legitimacy of the purpose of obtaining such secrecy and a strict procedure for disclosure of it to third parties tend to be required."[48]

In creating an environment in which criminal investigative procedures to obtain data held by companies are allowed to be implemented under the Code of Criminal Procedure, as described in **A** through **C** above, 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 by types in laws and regulations so that disclosures made in response to such procedures can be 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.

Establishment of new investigative procedures may be an issue to consider from a mid- to long-term perspective; in that case, 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 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.

(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 without obtaining consent from the Data Subject (Article 23, paragraph (1) of the same act). As an example of one category 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, whether a company provides personal information to

---

47 Ministry of Internal Affairs and Communications, *Comments on the Personal Information Protection Guidelines for Telecommunications Businesses (Public Notice of the Ministry of Internal Affairs and Communications No. 152 of 2017; Latest revision: Public Notice of the Ministry of Internal Affairs and Communications No. 297 of 2017)*], 3-5-1(1) (January 2019) (http://www.soumu.go.jp/main_content/000603940.pdf#page=60&zoom=100,0,822). There is a view that in the case of an inquiry concerning investigation-related matters, 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)).

48 Mikio Takashima, *Practice: Telecommunications Business Act*, p. 778 (NTT Publishing, 2015)

governmental bodies in accordance with an obligation imposed by a compulsory disposition based on a warrant or an inquiry concerning investigation-related matters, this is also understood as falling within the category of "cases based on laws and regulations."[49]

Establishment of new investigative procedures as stated in **A** through **C** above may be an issue to consider from a mid- to long-term perspective; in that case, 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, when establishing new procedures, it would be an option to subdivide and refine the procedures for investigative 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. When exploring this direction, it is expected that discussions will continue in the future towards the design of more appropriate legal systems, for example, in which different levels of due process of law are specified in accordance with the risk of invasion of privacy and the nature of data.[50]

(c) Act on the Protection of Personal Information Held by Administrative Organs, and Ordinances on the Protection of Personal Information

As investigative techniques for obtaining data are further utilized in Japan, a larger volume of personal information will be accumulated within investigative authorities. Therefore, we believe it is necessary to consider ideal approaches for regulation of the use and storage of such information.

For example, the Act on the Protection of Personal Information Held by Administrative Organs has already specified a Data Subject's right to request disclosure of its personal information held by administrative organs (Article 12, paragraph (1) of the same act), right to request correction (Article

---

49 For the view that in the case of receiving an inquiry concerning investigation-related matters, 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)*, pp. 45 and 29 (January 2019) (https://www.ppc.go.jp/files/pdf/190123_guidelines01.pdf), Personal Information Protection Committee, *Q & A Concerning "Guidelines Concerning the Act on the Protection of Personal Information" and "Responses in the Case of Leakage of Personal Data"*, Q5-17, A5-17 (June 7, 2019) (https://www.ppc.go.jp/files/pdf/1906_APPI_QA.pdf), and Katsuya Uga, *Commentary on the Act on the Protection of Personal Information (6th ed.)*, pp. 166-167 (Yuhikaku Publishing, 2018). Given this point, it can be said that the protection level provided to secrecy of communications under the Telecommunications Business Act is higher than that provided under the Act on the Protection of Personal Information (Tatsuhiko Yamamoto, *Protection of Personal Information on the Internet* in Shigeki Matsui et al., *Internet Law*, pp. 274, 295 (Yuhikaku Publishing, 2015)).

50 In that case, attention should be paid to the handling of information that does not constitute personal information under the Act on the Protection of Personal Information or secrecy of communications under Telecommunications Business Act but the protection level of which is high because there is a high risk of invasion of privacy (as a typical example, location information collected from mobile terminals used by consumers; Ministry of Internal Affairs and Communications, *Report by the Study Group for Handling of Location Information in the Case of Emergency: Location Information Privacy Report* (2014) (http://www.soumu.go.jp/main_content/000434727.pdf)).

27, paragraph (1) of the same act), and right to request suspension of use (Article 36, paragraph (1) of the same act). However, these rights can not be exercised over personal information pertaining to a judicial decision in a criminal case, etc. or a disposition executed by a public prosecutor, etc. (Article 45, paragraph (1) of the same act), and can not be exercised over personal information recorded in documents relating to trials and seized articles (Article 53-2, paragraph (2) of the Code of Criminal Procedure). In this respect, from a mid- to long-term perspective, it is expected that discussions will continue in the future regarding whether any right(s) similar to these rights should be applied to personal information collected or used in connection with criminal procedures.

In addition, it is necessary to consider ideal methods for regulation of the scope of the government's activities using information obtained for investigative purposes and on the period of storage of such information. 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, etc., 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 was subsequently found guilty.[51] Following this decision, law reform was effected by the Crime and Security Act 2010 in the United Kingdom to, among other matters, specify the period of storage of fingerprints, etc., of a suspect who was not found guilty.

From a mid- to long-term perspective, we consider that it is also beneficial to have a comprehensive understanding of the regulations applicable when data is obtained for investigative purposes and the regulations applicable to the use and storage of data after being obtained and, on the basis of that understanding, to seek a balance between both sets of legal provisions.[52]

For the future, it will also be necessary to advance discussions toward the development of required organizations and legal systems from a viewpoint of developing national security systems pertaining to use and storage of data.[53]

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

Even if investigative authorities obtain necessary data, issues still exist regarding the use of such data for trials. These issues have not been resolved by existing laws.

Courts need means to 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

---

51 *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)

52 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. 89, 93-98 (Shinzansha, 2017)

53 George Shishido et al., *Present and Future of Information Legislation*, Ronkyu Jurist, vol. 20, p. 179 (2017) [George Shishido]

and correctness of the data.[54] The Rules on Analysis of Information Technology (情報技術の解析に関する規則), established by the National Public Safety Commission, which is the governmental body which administers the National Police Agency of Japan, 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."

We believe that investigative authorities could include the analysis of the data in evidence together with the data, and submit a report on the analysis results for trials. We assume that such a report on the analysis results would contain the place where the analysis was conducted, the model number and product number of the subject recording medium, the hash values[55] 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.

However, even if the courts attempt to confirm the records regarding the investigation process and examine Japanese investigation officials regarding the procedures used and custody of the data, no criteria has been established for determining whether the process was appropriate, and courts may struggle to evaluate the admissibility or probative value of evidence. Therefore, we believe that 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 technological evolution.[56]

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.[57] 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 investigative authorities' requests, to the extent that these functions will not impose an excessive burden.

---

54 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 correctness 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 (成瀬剛 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)).

55 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.

56 Commentaries regarding the correctness of the digital forensic analysis include the NPO Institute of Digital Forensics, *Guidelines for Preservation of Evidence: 7th Edition* (July 20, 2018) (https://digitalforensic.jp/wp-content/uploads/2018/07/guideline_7th.pdf), and Eitaro Hamuro & Kiyoshi Kuniura, *Introduction to Digital Forensics* (Tokyo Horei Publishing, 2015).

57 If it is possible to confirm the hash values on the server 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.

3. Issues of Encrypted Data

In situations where investigative 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 Suspect

The right not to testify against oneself (privilege against self-incrimination; Article 38 of the Constitution of Japan) may be an issue where an investigative authority compels a suspect to disclose a password for encrypted data or to decrypt encrypted data.[58]

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 investigative 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 and whether or not the government already had knowledge of whether or not the suspect was capable of accessing or decrypting the data or whether incriminating data actually existed.[59] In another case, the ruling focused on whether accepting the request itself had an element that constituted "testifying."[60]

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 investigative 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).[61]

---

58 In cases where a suspect's face or fingerprint information is necessary to unlock a fingerprint authentication system or face authentication system, investigative 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.

59 *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).

60 *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).

61 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 but 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)

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.[62]

(2) Relationship with Third Party Other Than Suspect

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 investigative 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.[63] 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, investigative 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)).

In Australia, as a result of the enactment of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 in December 2018, investigative 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 bill).[64]

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 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,[65] 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

---

62 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)).

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

64 Parliament of AUSTRALIA, *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* (https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6195).

65 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.

to decrypt data,[66] 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.[67]

V. Obtaining Data Stored Overseas for Investigative Purposes

We must also consider issues concerning the principles of international law when domestic investigative 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 a Japanese investigative authority seeks data stored on foreign servers, the territorial scope of Japan's Code of Criminal Procedure is understood to include the countries where such servers are located.[68] However, questions remain as to whether such conducts infringe the sovereignty or jurisdiction of other foreign states.[69]

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.[70] This "national jurisdiction" is divided into three sub-concepts: (i) legislative jurisdiction, which authorizes

---

66 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 (2019), available at https://www.justice.gov/opa/press-release/file/1153446/download.

67 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)).

68 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 (ed.), *Exemplified Code of Criminal Procedure I*, pp. 5 and 10-12 (Seirin Shoin, 2012).

69 Council of Europe Cybercrime Convention Committee (T-CY), *Transborder access and jurisdiction: What are the options?,* Doc no T-CY (2012)3, 6 (2012).

70 Soji Yamamoto, *International Law (New Edition)*, p. 231 (Yuhikaku Publishing, 1994).

a legislative body to enact a domestic law or regulation and in so doing define the scope of 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.[71]

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.[72] In addition, some consider that a "substantial and genuine connection"[73] 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,[74] 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[75] the federal court relied it decisions 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. investigative 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.[76]

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

---

71 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).

72 Hironobu Sakai et al., *International Law*, p. 86 (Yushikaku Publishing, 2011).

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

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

75 *U.S. v. Aluminum Co. of America*, 148 F.2d 416 (1945).

76 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 (2017).

States, which indicates that a "genuine connection" between a country and the subject phenomenon 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.[77]

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

[77] Restatement (Fourth) of the Foreign Relations Law of the United States§ 407 (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.[78]

B. Cyberspace and Sovereignty

As for the relationship between cyberspace and sovereignty, the Tallinn Manual 2.0[79] 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 (cables, routers, servers, personal computers, etc.) located in their territory, and over any operations of that cyber infrastructure,[80] 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.[81]

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

As stated in section **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 investigative authority 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 investigative 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 investigative authority obtains data stored on a server located overseas via electronic network, even though the investigative 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.

A. Seeking Data Submission from Server-Managing Entities

Investigative authorities' access of data stored overseas via data production orders issued to a server-managing entity can take the form of either (i) when the investigative authorities order the relevant domestic company to submit data stored in a foreign country (e.g., seizure based on an order to produce, as described in **IV.1.(1)**),[82] or (ii) when the investigative authority directly orders foreign server managing entities, etc., to submit data held by such foreign operators located in a foreign state. They can be analyzed under international law as below.

[78] 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 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).

Article 3 of the proposed EU directive on e-evidence suggests that when a service provider is not established in the EU, EU member states shall ensure that such service provider offering services on their territory designates 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 should be addressed to such legal representative present in the EU. Thus, we can say that under EU law, whether the service provider provides service aimed at EU users is a factor in deciding whether a link exists with the service provider, and EU law ensures the effective exercise of jurisdiction by obligating a non-EU service provider to appoint a legal representative present in the EU territory (European Commission, *Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL laying down harmonized rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings* COM/2018/226 final - 2018/0107 (COD), available at https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1524129181403&uri=COM:2018:226:FIN).

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 conclude 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 issued by Korean investigative 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 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)).

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

---

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.

79 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.

80 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 on territory and involve objects, or are conducted by persons or entities, over which States may exercise their sovereign prerogative (*ibid*. 12).

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

82 As stated in **IV.1.(1)**, in Japan, a "seizure based on an order to produce a copy of records" is a system that enables investigative 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. 54, 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 investigative authority, that recording action, including accessing data located in a foreign country, is part of the investigative 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 to 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 investigative authority physically enters the territory of another state to conduct investigations and enforce their jurisdiction.[83]

On the other hand, with regard to (ii), when an ordering country's investigative authority directly requests a server-managing entity that 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 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 investigative authority attempts to obtain data by directly accessing a server located in a foreign country, as in the case of Japan's statutory Remote Access .

---

83 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 a view explicitly accepting 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 a view 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 78 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 seem 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. (http://jure.juridat.just.fgov.be/pdfapp/download_blob?idpdf=N-20151201-1; 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* **V.2.(2)A** below).

As stated above, a country's exercise of its sovereignty in another country's territory constitutes an infringement of territorial sovereignty except if made "pursuant to permissible rules derived from an international custom or treaty."[84]

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 investigative authority physically entering into a foreign country. Due to this absence of physical presence of the investigative authority in a foreign country, it could be said that remote access does not constitute enforcement measures enforcing the jurisdiction "in the territory of a foreign country." However, as a matter of international law, opinions on this issue are divided.[85] [86]

Therefore, as mentioned in Section **V.2(2)** below, in light of the need for such trans-border investigation of foreign stored data, the draft Second Additional Protocol to the Convention of Cybercrime seeks to justify, under international law, investigative methods that enable investigative authorities to obtain data through direct access to servers located in foreign countries, without being

---

84 S.S. Lotus (Fr. v. Turk.), 1927 P.C.I.J. (ser. A) No. 10 at 18-19 (Sep. 7).

85 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). There are also foreign court decisions permitting remote access to data stored in a foreign country. Examples include: a court decision allowing a Korean investigative 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 investigative 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)).

86 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.

restricted to the conventional principles of territorial sovereignty.[87] In this regard, Article 32 of the Convention on Cybercrime provides criteria under which investigative authorities are permitted to directly access data stored on a server located in a foreign country. However, Article 32 is only applicable between parties to the Convention on Cybercrime, meaning that such trans-border access to data is on principle premised on the consent of both the country where the relevant server is located and the relevant Data Subject, and Article 32 cannot be used to justify such investigations where consent is not obtained from the country where the server is located.

There is no established view in Japan in respect of remote access; discussions on this topic should be pursued in more depth.

To begin with, in Japan, while the legislators who introduced Remote Access 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 investigative authorities should refrain from conducting Remote Access involving a server which is clearly located in a foreign country and, instead, rely on mutual legal assistance between countries.[88]

The position above has become a subject of discussion in criminal cases before the Japanese courts. However, no definite view has been presented regarding how to evaluate the necessity and desirability of relying on MLATs rather than remote access if there is a possibility that target data is stored on a

---

87 Commentary notes that, in the U.S., the traditionally-adopted view is that the existence of any separate international procedure, such as MLATs, will not necessarily restrain the exercise of jurisdiction over a foreign country (Yukari Ishii, *International Regulation over Cross-border Crimes*, pp. 88-104 and 175-197 (2017)).

88 *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).

server located in a foreign country. The emerging position seems to be that remote access should not be rejected outright in such situations.[89]

In Japanese academia, it has been noted that it would become impossible for investigative authorities to continue their investigations if it is necessary to resort to MLATs even in situations where the location of the server is unknown; therefore, investigative 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.[90] 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.[91]

(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

---

89 Yokohama District Court, Judgment, March 17, 2016, LEX/SB25542385, appears to urge careful consideration for the use of Remote Access, holding that "because there was a good possibility that the server computer was located in a foreign country, and the investigative authority was aware of that possibility, it is fair to say that the investigative authority should, in principle, have refrained from taking such measure." The related appellate decision, Tokyo High Court, Judgment, December 17, 2016, Kokeishu [*High Court Criminal Case Report*], vol. 69, no. 2, p. 5, held that "since there was a possibility that the server was located in a foreign country, it can be said that the investigative authority should have resorted to international assistance with investigation or similar investigative techniques." Subsequently, Osaka High Court, Judgment, September 11, 2018, LEX/DB25449705 (an appeal pending before the Supreme Court), merely noted that "in a situation where it has become clear that storage media from which an electromagnetic record should be copied is located within the territory of a foreign country, if Article 32 of the Convention [on Cybercrime] does not permit resorting to [remote] access or similar measures, then considering that there is a possibility that issues regarding that foreign country's sovereignty may arise, there are a considerable amount of people who point out that it is advisable to refrain from taking that measure, and to obtain the consent of the foreign country or to request international assistance with the investigation." In addition, Tokyo High Court, Judgment, January 15, 2019, L07420003 (an appeal pending before the Supreme Court), held that "in order to conduct Remote Access in the above situation, it is advisable to request international mutual legal assistance. However, it is fair to say that conducting Remote Access without requesting international mutual legal assistance may possibly give rise to a diplomatic problem, but, nevertheless, will not immediately affect the determination as to the lawfulness of the investigation under the Japanese Criminal Procedure Law." With respect to the admissibility of evidence, the Tokyo High Court decision above further held that whether the Remote Access was conducted without requesting international mutual legal assistance is not a factor to be considered "in determining the admissibility of the evidence." A Supreme Court ruling is awaited regarding this issue in Japanese criminal law proceedings.

90 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).

91 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).

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 EU General Data Protection Regulation (EU/2016/679) (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.[92] Moreover, a joint answer of the European Data Protection Supervisor (EDPS) and the European Data Protection Board (EDPB), addressed to European Parliament's Committee on Civil Liberties, Justice and Affairs (LIBE Committee), indicates that the CLOUD Act conflicts with Article 48 of the GDPR and emphasizes the importance of concluding a comprehensive agreement between the EU and the U.S. regarding access to electronic evidence.[93]

However, in principle, each country has discretion to determine what laws to enact within the scope of its legislative jurisdiction. We cannot say that there are any established international legal principles regarding a method to coordinate conflict of laws that exists between two or more treaty signatory countries.[94]

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.2** above, the CLOUD Act provides that if certain requirements are met, the 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.[95] Comity, as a matter of general international law, cannot escape from ambiguity that may arise in the extension of a comity judgment, and issues remain as to whether or not a problem exists in a comity judgment from a foreseeability perspective and as to whether or not a comity judgment tends 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.

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

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

---

92 European Parliament, "Adequacy of the protection afforded by the EU-US Privacy Shield European 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

93 EPDB-EDPS Joint Response to the LIBE Committee on the impact of the US Cloud Act on the European legal framework for personal data protection, *available at* https://edpb.europa.eu/our-work-tools/our-documents/letters/epdb-edps-joint-response-libe-committee-impact-us-cloud-act_en

94 Hironobu Sakai et al., *International Law*, p. 86 (Yuhikaku Publishing, 2011).

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

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 an investigative authority 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 investigative authority (*e.g.*, the Ministry of Justice of Japan) to directly request assistance from a relevant authority in the target country (*e.g.*, the U.S. Department of Justice) without using the above mentioned diplomatic channels.[96]

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.[97] Critics state that the time and effort required to use the MLAT procedures prevent expeditious collection of evidence.[98] Moreover, if the investigative authorities cannot identify the 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.[99]

(2) The Convention on Cybercrime

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.[100]

---

96 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.

97 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).

98 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)

99 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).

100 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).

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

A. Data Production Orders (Article 18)

With respect to issuing data production orders to entities or persons located within the territory of the investigating country, Article 18 of the Convention on Cybercrime requires member countries to take necessary legislative and other measures to authorize the investigative authorities to order:[101]

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 Party'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 Party's territory.[102] 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 assumes situations where the targeted computer data is stored in a foreign country and whether we can interpret the member countries as having agreed that an order for submission of data is permissible in such situations.[103]

Therefore, the draft Second Additional Protocol to the Convention of Cybercrime seeks to set up criteria for the exercise of jurisdiction in situations where the location of data storage is unclear, as explained in **Section V.2(2)C** below.

---

101 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).

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

103 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).

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 Subject (including the relevant service providers, if the server managers have the contractual authority to disclose the stored data) (item (b) of the same article).[104]

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.[105]

In addition, the drafters of the Convention did not consider item (b) of Article 32 to authorize or preclude situations beyond this article. Therefore, additional solutions may be agreed upon at a later stage.[106]

C. The Draft Second Additional Protocol

The Council of Europe Cybercrime Convention Committee is negotiating the draft Second Additional Protocol, with a view to its adoption in December 2022.[107]

---

104 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 placed by that Data Subject in a foreign country, provided that they have the lawful authority, and voluntarily submits the relevant e-mail to an investigative 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 police access the account and if the police are sure that the data of the mailbox is located with another Party, police 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)).

105 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).

106 Council of Europe Cybercrime Convention Committee (T-CY), *Transborder access and jurisdiction: What are the options?*, Doc No T-CY (2012)3 , 27 (2017).

107 Council of Europe Cybercrime Convention Committee (T-CY), *Preparation of the 2nd Additional Protocol to the Budapest Convention on Cybercrime State of play Note by the Chair for the attention of the 21st Plenary of the T-CY*, 4 (2019), *available at* https://rm.coe.int/t-cy-2019-19-protocol-tor-extension-chair-note-v3/16809577ff

While the draft Second Additional Protocol makes use of mutual investigative assistance as the basis for trans-border investigations, it provides that a provider's direct assistance should be utilized as an auxiliary measure, and includes a policy of clarifying legal frameworks and implementing safety measures, including data protection.[108] In particular, with regard to a provider's cooperation, it is worth noting that there is a proposal citing the need for a legal framework which sets out conditions and procedures to provide adequate explanation to cloud service providers, and that such explanation should adequately protect rights under personal data protection and criminal procedure regulations of each country.[109]

With regard to investigation methods not covered by item (b) of this article, namely, trans-border access to data without consent from the Data Subject, the Council of Europe Cybercrime Convention Committee (T-CY) Cloud Evidence Group is considering the authorization of trans-border access to data stored in a server located in a foreign country (i) when the investigative authority uses lawfully obtained credential information (i.e., user IDs, passwords, etc.), or (ii) in emergency or other circumstances, such as those involving imminent danger, physical harm, destruction of relevant evidence, the escape of a suspect, or similar matters.[110] Given the limitations on applying traditional territoriality principles to cyberspace, the Cloud Evidence Group also makes a noteworthy suggestion regarding how the principles of jurisdiction should operate with regard to an investigation to obtain data stored in a foreign county. Where the place of data storage is uncertain, such as where the location of data storage changes frequently or where one set of data is divided and dispersed among various storage locations, it is not appropriate to rely on the tenet of the territoriality principle that holds that enforcement jurisdiction is limited to the territory of a country where the relevant data is stored. In such case, it is suggested that if there is a justifiable connection between the person with the right to exclusively dispose of the relevant data and the relevant state (*see* **1.(1)A** above), such

---

108 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. 54 (2019); Council of Europe Cybercrime Convention Committee (T-CY), *Criminal Justice access to data in the cloud: Cooperation with "foreign" service providers, T-CY (2016)*, 2 (2016).

109 Council of Europe Cybercrime Convention Committee (T-CY) Cloud Evidence Group, *Criminal justice access to data in the cloud: Recommendations*, 44 - 46 (2016).

110 Council of Europe Cybercrime Convention Committee (T-CY) Cloud Evidence Group, *Criminal justice access to data in the cloud: Recommendations*, 44-45 (2016); Spoenle, *Cloud computing and cybercrime investigations: territoriality vs the power of disposal* discussion paper, Project on Cybercrime, Council of Europe, Strasbourg, 11 (2010). https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa3df.

country's investigative authority is able to exercise enforcement jurisdiction over the data or storage media thereof.[111]

(3) US-UK Executive Agreement

An executive agreement under the CLOUD Act has 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 concluded an executive agreement. On October 3, 2019, the U.S. and the U.K. concluded the US-UK Executive Agreement (**III.2** above).

Under the agreement between the U.S. and the U.K., either country is able to request the submission from a service provider in the other country of data pertaining to serious criminal offence under the law of the country where the investigative authority is located (Sections 1, 4, and 5 of the agreement). However, the U.K. has the right under the executive agreement to deny the use of the relevant data for 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 (Section 8.4 of the agreement).

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

1. Functions of an Executive Agreement

As stated in **III.2** above, the functioning of the CLOUD Act depends upon the U.S. government and a foreign country government concluding 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)**).[112]

---

111 In principle, enforcement jurisdiction can be exercised only within the territory of the country vested with jurisdiction. Under MLATs, the country of the investigative authority must request assistance from the relevant authorities in the country where the investigation is conducted. However, if the place of storage of the relevant data is unidentifiable by the investigative authority, it cannot be determined which country has the right to exert sovereignty over the data. Therefore, investigative authorities in many countries may experience situations where they must directly access data located in an unknown place. In this respect, if a particular country has jurisdiction over the person with the "power of disposal" or "person in possession or control" over the relevant data, namely, if a particular country has a justifiable connection with the person having the right to exclusively dispose of the data (such as modifying, deleting, or making the data unusable), that country should be able to access the data belonging to that person or entity without the consent of the country where the data is located (Council of Europe Cybercrime Convention Committee (T-CY) Cloud Evidence Group, *Criminal justice access to data in the cloud: Recommendations*, 44-46 (2016)).

112 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.

Below, we will first highlight specific issues under Japanese law that may arise in situations where the U.S. government orders a Japanese business operator to submit data under the CLOUD Act.[113] Then, with these issues in mind, we will discuss the points that should be considered when Japan decides to conclude an executive agreement with the U.S.

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

(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 constitute a criminal infringement of the secrecy of those communications (Article 179 of the Telecommunications Business Act). In this respect, it is necessary to consider, for example, whether or not the disclosure is 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,[114] compliance with a foreign warrant could not be justified as an Act Performed in Accordance with Laws and Regulations.

---

113 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.

114 *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).

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 country.[115] 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 must 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.

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 information to third parties without the consent of the Data Subject (Article 23, paragraph (1) 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.[116]

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

---

115 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) [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 in a foreign country, and even if the person with managing authority over the server is located in a foreign country 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).

116 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)

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 is likely to violate the Act on Protection of Personal Information.

3. Points to Note in Designing an Executive Agreement

As a preliminary note, in Japan, given Ohira's Three Principles,[117] an executive agreement based on the CLOUD Act would be considered a "treaty," the adoption of which requires the approval of the Diet.[118] In addition, if Japan enters into discussions with the U.S. to conclude an executive agreement, it is necessary to consider the following points in designing the executive agreement.[119]

(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.[120] For example, in order to obtain a subpoena under U.S. law, only the existence of a reasonable suspicion is

---

117 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 legal matter (for example, a situation where it becomes necessary to implement a new legislative measure due to the conclusion of the international agreement), (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 applicable 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).

118 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)).

119 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.

120 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/).

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 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"[121] and "serious crime."[122] 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.[123]

(3) Protection of Japanese Persons

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.[124] 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 located in the other (Section 4.3 of the same agreement), and a similar provision could be included in a US-Japan executive agreement.

(4) Impact on Other International Agreements

As a result of the conclusion 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 concluded by Japan. For example, the adequacy decision to Japan based 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 the Japanese government and the U.S. government should be conducted while maintaining an adequately high level of protection for personal information.[125]

---

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

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

123 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 (Section 1.14 of the same agreement).

124 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.

125 On January 23, 2019, Japan received an adequacy certification 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.

(5) Adjustment of Domestic Laws and Regulations

In addition to the conclusion of an executive agreement, it would be necessary to adjust Japanese law 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.

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

Data-possessing companies in Japan and foreign countries have begun to issue transparency reports, which publicize their response policies, current status, 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 not only their policies for responding to requests made by governmental bodies, but also 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; response policy
B	Breakdown of user information disclosure/deletion requests; number of responses; response rate; response policy
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; response policy
F	Breakdown of user information disclosure/deletion requests; number of responses; response rate; response policy

Among Japanese companies, awareness is gradually spreading that it is an important task to ensure transparency in responding to access requests. At the present, however, transparency reports are only publicized by a very limited number of companies.

It is considered possible for Japanese companies, in the future, to accumulate and publicize information about their responses to governmental bodies' disclosure requests, in order to improve their transparency, thereby promoting the protection of Data Subjects and obtaining the understanding of civil society, and also in order to achieve appropriate cooperation with investigations. Those efforts may give a sense of security to Data Subjects, namely, users of services provided by those companies. Also, it is fair to say that those efforts will improve each company's corporate image in civil society and would 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, that is, how to design a user friendly, easy-to-understand report.

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) and the United States-Mexico-Canada Agreement (USMCA = NAFTA 2.0), embody the core principle of the free transfer of data.

However, as more concerns over the effectiveness of data law enforcement are raised as a result of active cross-border data transfer, it follows instead that widespread data localization ought to be permitted and this in turns runs the risk of reversing the current trend towards the promotion of cross-border data transfer. In light of this, it is important to ensure that investigative authorities can have access to data located in foreign countries to the extent necessary and adequate.

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

The "Operational Approach" formulated by the Data & Jurisdiction Working Group of the Internet & Jurisdiction Policy Network, a multi-stakeholder organization which engages in research studies about cross-border data acquisition for investigative purposes, presents (i) the CLOUD Act, (ii) the proposal for an e-evidence directive and regulation in the EU, 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.[126]

In this respect, 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, a timely adoption of proposed additional protocol to the Convention on Cybercrime mentioned above is desirable. At the same time, in terms of promptness and feasibility, like-minded countries that share a common sense of values should take the initiative and steadily formulate a framework of agreements in accordance with the spirit of the DFFT. Accordingly, from the point of view above, it would be worthwhile for Japan to consider the necessary legal issues, with a view to concluding a bilateral international agreement, as envisaged by the CLOUD Act.

End

---

126 Internet & Jurisdiction Policy Network, *Concrete Proposals for Operational Norms, Criteria and Mechanisms* (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 so-called "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).