[Translation ver.1]

Nishimura Institute of Advanced Legal Studies

Report by the "CLOUD Act Study Group"

Reference Material: Collection of Relevant Provisions

I. CLOUD Act[1] (→ III, IV, VI)

SEC. 103. PRESERVATION OF RECORDS; COMITY ANALYSIS OF LEGAL PROCESS.

(a) REQUIRED PRESERVATION AND DISCLOSURE OF COMMUNICATIONS AND RECORDS.—

(1) AMENDMENT.—Chapter 121 of title 18, United States Code, is amended by adding at the end the following:

"§2713. Required preservation and disclosure of communications and records

"A provider of electronic communication service or remote computing service shall comply with the obligations of this chapter to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States.".

(2) [Omitted]

(b) COMITY ANALYSIS OF LEGAL PROCESS SEEKING CONTENTS OF WIRE OR ELECTRONIC COMMUNICATION.—Section 2703 of title 18, United States Code, is amended by adding at the end the following:

"(h) COMITY ANALYSIS AND DISCLOSURE OF INFORMATION REGARDING LEGAL PROCESS SEEKING CONTENTS OF WIRE OR ELECTRONIC COMMUNICATION.—

"(1) [Omitted]

"(2) Motions to quash or modify.—

(A) A provider of electronic communication service to the public or remote computing service, including a foreign electronic communication service or remote computing service, that is being required to disclose pursuant to legal process issued under this section the contents of a wire or electronic communication of a subscriber or customer, may file a motion to modify or quash the legal process where the provider reasonably believes—

"(i) that the customer or subscriber is not a United States person and does not reside in the United States; and

"(ii) that the required disclosure would create a material risk that the provider would violate the laws of a qualifying foreign government. [Omitted]

"(B) Upon receipt of a motion filed pursuant to subparagraph (A), the court shall afford the governmental entity that applied for or issued the legal process under this section the

---

[1] Clarifying Lawful Overseas Use of Data Act, *available at* https://www.justice.gov/dag/page/file/1152896/download)

opportunity to respond. The court may modify or quash the legal process, as appropriate, only if the court finds that—

"(i) the required disclosure would cause the provider to violate the laws of a qualifying foreign government;

"(ii) based on the totality of the circumstances, the interests of justice dictate that the legal process should be modified or quashed; and

"(iii) the customer or subscriber is not a United States person and does not reside in the United States.

"(3)~(5) [Omitted]"

(c) RULE OF CONSTRUCTION.—Nothing in this section, or an amendment made by this section, shall be construed to modify or otherwise affect the common law standards governing the availability or application of comity analysis to other types of compulsory process or to in stances of compulsory process issued under section 2703 of title 18, United States Code, as amended by this section, and not covered under subsection (h)(2) of such section 2703.

SEC. 104. ADDITIONAL AMENDMENTS TO CURRENT COMMUNICATIONS LAWS.

Title 18, United States Code, is amended—

(1) in chapter 119—

(A) in section 2511(2), by adding at the end the following:

"(j) It shall not be unlawful under this chapter for a provider of electronic communication service to the public or remote computing service to intercept or disclose the contents of a wire or electronic communication in response to an order from a foreign government that is subject to an executive agreement that the Attorney General has determined and certified to Congress satisfies section 2523." and;

(B) [Omitted]

(2)~(3) [Omitted]

SEC. 105. EXECUTIVE AGREEMENTS ON ACCESS TO DATA BY FOREIGN GOVERNMENTS.

(a) IN GENERAL.—Chapter 119 of title 18, United States Code, is amended by adding at the end the following:

"§2523. Executive agreements on access to data by foreign governments

"(a) [Omitted]

"(b) Executive Agreement Requirements.—For purposes of this chapter, chapter 121, and chapter 206, an executive agreement governing access by a foreign government to data subject to this chapter, chapter 121, or chapter 206 shall be considered to satisfy the requirements of this section if the Attorney General, with the concurrence of the Secretary of State, determines, and submits a written certification of such determination to Congress, including a written certification and explanation of each consideration in paragraphs (1), (2), (3), and (4), that—

"(1) the domestic law of the foreign government, including the implementation of that law, affords robust substantive and procedural protections for privacy and civil liberties in light of the data collection and activities of the foreign government that will be subject to the agreement, if—

"(A)~(B) [Omitted]

"(2) the foreign government has adopted appropriate procedures to minimize the acquisition, retention, and dissemination of information concerning United States persons subject to the agreement;

"(3) the terms of the agreement shall not create any obligation that providers be capable of decrypting data or limitation that prevents providers from decrypting data; and

"(4) the agreement requires that, with respect to any order that is subject to the agreement—

"(A) the foreign government may not intentionally target a United States person or a person located in the United States, and shall adopt targeting procedures designed to meet this requirement;

"(B)~(C) [Omitted]

"(D) an order issued by the foreign government—

"(i) shall be for the purpose of obtaining information relating to the prevention, detection, investigation, or prosecution of serious crime, including terrorism;

"(ii)~(vi) [Omitted]

"(E)~(K) [Omitted]

"(c) [Omitted]

"(d) EFFECTIVE DATE OF CERTIFICATION.—

"(1) NOTICE.—Not later than 7 days after the date on which the Attorney General certifies an executive agreement under subsection (b), the Attorney General shall provide notice of the determination under subsection (b) and a copy of the executive agreement to Congress, including—

"(A)~(B) [Omitted]

"(2) ENTRY INTO FORCE.—An executive agreement that is determined and certified by the Attorney General to satisfy the requirements of this section shall enter into force not earlier than the date that is 180 days after the date on which notice is provided under paragraph (1), unless Congress enacts a joint resolution of disapproval in accordance with paragraph (4).

"(3) [Omitted]

"(4) CONGRESSIONAL REVIEW.—

"(A) [Omitted]

"(B) JOINT RESOLUTION ENACTED.—Notwithstanding any other provision of this section, if not later than 180 days after the date on which notice is provided to Congress under paragraph (1), there is enacted into law a joint resolution disapproving of an executive agreement under this section, the executive agreement shall not enter into force.

"(C) [Omitted]

"(5)~(8) [Omitted]

"(e)~(h) [Omitted]"

(b) [Omitted]

II. Japanese Laws

(i) Constitution of Japan[2] (→ IV, VI)

Article 31 (Guarantee of Life and Liberty and Restrictions on Criminal Penalties)

No person will be deprived of life or liberty, nor will any other criminal penalty be imposed, except according to procedure established by law.

Article 35 (Restrictions on Entry, Search, and Seizure)

(1) The right of all persons to be secure in their homes, papers and effects against entries, searches and seizures will not be impaired except upon warrant issued for an adequate cause and particularly describing the place to be searched and things to be seized, or except as provided by Article 33.

(2) Each search or seizure will be made upon separate warrant issued by a competent judicial officer.

Article 38 (Prohibition of Confession under Compulsion and Limitation on Admissibility in Evidence of Confession)

(1) Confession made under compulsion, torture, or threat, or after prolonged arrest or detention will not be admitted in evidence.

(2)~(3) [Omitted]

(ii) Code of Criminal Procedure[3] (→ IV)

Article 53-2 (Exclusion from Application)

(1) [Omitted]

(2) The provisions of Chapter IV of the Act on the Protection of Personal Information Held by Administrative Organs (Act No. 58 of 2003) and Chapter IV of the Act on the Protection of Personal Information Held by Independent Administrative Agencies, etc. (Act No. 59 of 2003) do not apply to personal information recorded in documents relating to trials and seized articles.

(3)~(4) [Omitted]

Article 99 (Seizure, Submission Order)

(1) [Omitted]

(2) When the article to be seized is a computer, and a recording medium is connected via telecommunication lines to that computer and is in the condition that enables the finding that the recording medium is used to retain electronic or magnetic records that have been prepared or altered on that computer or electronic or magnetic records that can be altered or erased on that

---

[2] Constitution of Japan of 1946. The article headings of the Constitution of Japan are according to the website of the House of Representatives (http://www.shugiin.go.jp/internet/itdb_annai.nsf/html/statics/shiryo/dl-constitution.htm#3sho).

[3] Act No. 131 of 1948. The article headings are according to 宇賀克也ほか編『六法全書 平成 31 年版』[Katsuya Uno et al. (ed.), *Statutes Book 2019*] (Yuhikaku Publishing, 2019).

computer, 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.

(3) [Omitted]

Article 99-2 (Seizure by an Order to Produce a Copy of Records)

The court may, when it is necessary, conduct a Seizure by an Order to Produce a Copy of Records (meaning having a custodian of electronic or magnetic records or a person with the authority to access electronic or magnetic records copy the necessary electronic or magnetic records onto a recording medium or print said records out, and seizing said recording medium; the same applies hereinafter).

Article 100 (Seizure of Postal Items)

(1) The court may seize or order the submission of postal items, items of correspondence, or documents sent by telegraph sent to or from the defendant that, based on the provisions of laws and regulations, are held in the custody of or are in the possession of a person who handles communications.

(2) The postal items, items of correspondence, or documents sent by telegraph sent to or from the defendant that, based on the provisions of laws and regulations, are held in the custody of or are in the possession of a person who handles communications, but are not subject to the preceding paragraph, may be seized or their submission ordered only when they can be reasonably supposed to be related to the case charged to the court.

(3) When the court makes a disposition under the preceding two paragraphs, the sender or recipient must be so notified; provided however, that this does not apply when there is a concern that such notification would obstruct court proceedings.

Article 110 (Manner of Execution)

A seizure warrant, warrant for Seizure by an Order to Produce a Copy of Records, or search warrant must be presented to the person subject to the disposition.

Article 110-2 (Manner of Execution of Seizure of Recording Media Containing Electronic or Magnetic Records)

If the article to be seized is a recording medium containing electronic or magnetic records, the person executing the seizure warrant may take the measures set forth in the following items in lieu of seizure; the same applies when a seizure is made in an open court:

(i) to copy the electronic or magnetic records recorded on the recording medium which is to be seized onto some other recording medium, print them out, or transfer them, and to seize that other recording medium; and

(ii) to have the person subject to the seizure copy the electronic or magnetic records recorded on the recording medium which is to be seized onto some other recording medium, print them out, or transfer them, and to seize that other recording medium.

Article 114 (Attendance of a Responsible Person)

(1) When executing a seizure warrant, warrant for Seizure by an Order to Produce a Copy of Records, or search warrant in a public office, the executing officer must notify the head of the office or his or her deputy of the execution, and have that head or deputy attend it.

(2) Except for the cases subject to the preceding paragraph, when executing a seizure warrant, warrant for Seizure by an Order to Produce a Copy of Records, or search warrant in the residence of a person or in a house, building, or vessel guarded by a person, the executing officer must have the residence owner, the guard, or his or her deputy attend the execution. If unable to have any such person so attend, then the executing officer must have a neighbor or an official of the local government attend the execution.

Article 197 (Examination Necessary for Investigation)

(1) With regard to an investigation, the necessary examinations may be conducted to achieve the objective of that investigation; provided, however, no compulsory disposition may be applied unless governed by special provisions established in this Code.

(2) Public offices or public or private organizations may be asked to make a report on necessary particulars relating to the investigation.

(3) When a public prosecutor, public prosecutor's assistant officer, or judicial police officer finds it necessary to execute a seizure or a Seizure by an Order to Produce a Copy of Records, that officer may specify the necessary electronic or magnetic records out of the electronic or magnetic records pertaining to the transmission source, the transmission destination, the date and time of the transmission, and other transmission history of electronic communications which are recorded in the course of business, may determine a time period not exceeding 30 days, and may request, in writing, that none of the electronic or magnetic records so specified be erased by a person engaged in the business of providing facilities for conducting electronic communications for use in the communications of other persons or by a person establishing facilities for conducting electronic communications capable of acting as an intermediary for the transmissions of many, unspecified persons for the purpose of that person's own business. In this case, if it is deemed no longer necessary to execute the seizure or the Seizure by an Order to Produce a Copy of Records with regard to the above-mentioned electronic or magnetic records, the officer must revoke the above-mentioned request.

(4) The time period of requested non-erasure pursuant to the preceding paragraph may be extended to a period not exceeding 30 days when it is particularly necessary; provided however, that the total time period of requested non-erasure may not exceed 60 days.

(5) When a request is made pursuant to paragraph (2) or paragraph (3), if it is necessary, a request may be made that the particulars relating to that request not be divulged without reason.

Article 218 (Seizure, Seizure by an Order to Produce a Copy of Records, Search, and Inspection upon Warrant)

(1) Public prosecutors, public prosecutor's assistant officers, or judicial police officials may, when it is necessary for the investigation of an offense, conduct a seizure, Seizure by an Order to Produce a Copy of Records, search, or inspection upon a warrant issued by a judge. In this case, a physical examination of a person must be conducted upon a warrant for physical examination.

(2) When the article to be seized is a computer, and a recording medium is connected via telecommunication lines to that computer and is in the condition that enables the finding that the recording medium is used to retain electronic or magnetic records that have been prepared or altered on that computer or electronic or magnetic records that can be altered or erased on that computer, 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.

(3)~(6) [Omitted]

Article 219 (Form of Warrant for Seizure, etc.)

(1) The warrant mentioned in the preceding Article must contain the name of the suspect or defendant, the charged offense, the articles to be seized, the electronic or magnetic records to be recorded or to be printed out and the person who is to record them or print them out, the place, body, or articles to be searched, the place or articles to be inspected, or the person to be examined and the conditions regarding the examination of a person, the period of validity and a statement to the effect that the seizure, Seizure by an Order to Produce a Copy of Records, search, or inspection may not be commenced in any way after the lapse of the period of validity and that in this case the warrant must be returned to the court, the date of issue, and other particulars as prescribed in the rules of court; and the judge must affix his or her name and seal to it.

(2) In the case of paragraph (2) of the preceding Article, in addition to the particulars prescribed in the preceding paragraph, the warrant mentioned in the preceding Article must contain the scope to be copied out of the electronic or magnetic records with regard to the recording medium connected via telecommunication lines to the computer to be seized.

(3) [Omitted]

Article 222 (Provisions Mutatis Mutandis Applied Regarding Seizure, Search, and Inspection; Limitation on the Time of Inspection; Attendance of the Suspect; Sanctions over Those Who Refuse Physical Examination)

(1) Paragraph (1) of Article 99, Article 100, Articles 102 through 105, Articles 110 through 112, Article 114, Article 115, and Articles 118 through 124 apply mutatis mutandis to a seizure and a search conducted by a public prosecutor, public prosecutor's assistant officer, or a judicial police official pursuant to Article 218, Article 220, and the preceding Article, . . . ; provided, however, that the dispositions prescribed in Articles 122 through 124 may not be executed by a judicial constable.

(2)~(7) [Omitted]

(iii) Rules of Criminal Procedure[4] (→ IV)

Article 139 (Manner of Request for Warrant)

(1) A request for a warrant must be filed in writing.

(2) [Omitted]

[4] Rules of the Supreme Court No. 32 of December 1, 1948.

(iv) Code of Conduct for Criminal Investigation[5] (→ IV)

Article 108 (Prohibition of Voluntary Search in a Person's Residence)

If it is necessary to conduct a search in the residence of a person or in a house, building, or vessel guarded by a person, and even if it is found that voluntary consent is likely to be obtained from the residence owner or guard, a search permit must be obtained to conduct the search.

(v) Act on Communication Interception for Criminal Investigation[6] (→ IV)

Article 10 (Presentation of an Interception Warrant)

(1) An interception warrant must be presented to the communication manager, etc.; provided, however, that this does not apply to a summary of the alleged facts of the crime.

(2) [Omitted]

Article 14 (Interception for the Purpose of Determining Relevancy)

(1) If it is uncertain whether or not a communication made during the execution of an interception falls within the scope of communications to be intercepted as specified in the interception warrant (each an "Interceptable Communication"), the public prosecutor or judicial police officer may intercept that communication to the minimum extent necessary to determine whether or not it constitutes an Interceptable Communication.

(2) [Omitted]

Article 29 (Preparation of Interception Record)

(1) Each time when suspending or ending the execution of an interception (except under Article 20, paragraph (1), or Article 23, paragraph (1), item (ii); this applies below in this paragraph), the public prosecutor or judicial police officer must promptly prepare one record of the substance of the intercepted communications for the use of criminal proceedings. The same applies when the recording medium is changed or the recording thereon otherwise ends during the execution of the interception.

(2) Each time when suspending or ending the execution of a reproduction of communications, the public prosecutor or judicial police officer must promptly prepare one record of the substance of the reproduced communications for the use of criminal proceedings. The same applies when the recording medium is changed or the recording thereon otherwise ends during the execution of the reproduction.

(3) The record mentioned in paragraph (1) is prepared by deleting any communications other than those mentioned in the following items from the recording medium recorded pursuant to the second sentence of Article 24, paragraph (1) or Article 26, paragraph (2) or a duplication, prepared pursuant to Article 25, paragraph (3), of the recording medium mentioned in paragraph (1) of the same article:

(i) an Interceptable Communication;

---

5 Rules of the National Public Safety Commission No. 2 of 1957.

6 Act No. 137 of 1999.

(ii) a communication intercepted pursuant to Article 14, paragraph (2), which requires a measure to be taken to restore its substance;

(iii) a communication intercepted pursuant to Article 15 or Article 14, paragraph (2), which is found to constitute a communication mentioned in Article 15; and

(iv) a communication made on the same occasion as any communication set forth in any one of the preceding items.

(4) The record mentioned in paragraph (2) is prepared by deleting any communications other than those mentioned in the following items from the recording medium recorded pursuant to the second sentence of Article 24, paragraph (1) or Article 26, paragraph (2) or a duplication, prepared pursuant to Article 25, paragraph (3), of the recording medium mentioned in paragraph (2) of the same article:

(i) an Interceptable Communication;

(ii) a communication reproduced pursuant to Article 21, paragraph (4) (including cases handled according to the same paragraph under Article 23, paragraph (4)), which requires a measure to restore its substance;

(iii) a communication reproduced pursuant to Article 21, paragraph (5) (including cases handled according to the same paragraph under Article 23, paragraph (4)) and a communication reproduced pursuant to Article 21, paragraph (4), which is found to constitute a communication mentioned in Article 15; and

(iv) a communication made on the same occasion as any communication set forth in any one of the preceding items.

(5) ~ (7) [Omitted]

Article 30 (Notice to the Communicating Parties)

(1) The public prosecutor or judicial police officer must provide the parties to the communication recorded in the interception record with a written notice stating the fact of preparation of an interception record and the following matters:

(i) the time and date of the start and end of, and the name of the counter party (only if known) to, the communication;

(ii) the date of issuance of the interception warrant;

(iii) the start and end dates of the interception;

(iv) the means of communication subject to the interception;

(v) the name of crime and the applicable penal statute, which are stated in the interception warrant;

(vi) in respect of the communication mentioned in Article 15, that fact and the name of crime and the applicable penal statute pertaining to the relevant communication; and

(vii) that the party may make a request for permission of hearing, etc. (meaning hearing, inspection, or preparation of a duplicate; the same applies below in this item) of an interception record pursuant to the following article and a request for permission of hearing, etc. of the original interception record pursuant to Article 32, paragraph (1), and may enter an appeal pursuant to paragraph (1) or paragraph (2) of Article 33.

(2) The notice mentioned in the preceding paragraph must be dispatched within 30 days after the end of the interception except if the communication party is not identified or the whereabouts of such party is unknown. However, if a judge of the district court finds that the investigation is likely to be prevented, that judge may extend the time period for which a notice must be dispatched

pursuant to this paragraph by fixing a period of not more than 60 days, upon request of a public prosecutor or judicial police officer.

(3) [Omitted]

(vi) Act on the Use of Information and Communications Technology in Administrative Procedures[7] (→ IV)

Article 2 (Definitions)

As used in this Act, the terms set forth in each of the following items have the meaning specified in the relevant item:

(i)~(iii) [Omitted]

(iv) The term "signature, etc." means a signature, name, own signature, joint signature, seal, or other manners of affixing one's name to a document, etc.;

(v) [Omitted]

(vi) The term "application, etc." means an application, notification, or other manners of notice to an administrative agency based on the applicable laws and regulations (excluding those made in litigation procedures and other proceedings conducted by a judicial court as well as in proceedings based on the applicable laws and regulations pertaining to criminal cases as defined by Cabinet Order (being referred to as "judicial proceedings" below in the following item to item (ix)));

(vii)~(x) [Omitted]

Article 3 (Application, etc. by an Electronic Data Processing System)

(1)~(3) [Omitted]

(4) In a case falling under paragraph (1), an application, etc. to which a signature, etc. is required by other laws and regulations applicable to that application, etc. may be replaced, notwithstanding the provisions of those laws and regulations, by the administrative agency with an alternative name clarification measure as specified by Ministerial Order of the competent Ministry.

(vii) Telecommunications Business Act[8] (→ IV, VI)

Article 4 (Protection of Secrecy)

(1) The secrecy of communications handled by a telecommunications carrier must not be violated.

(2) [Omitted]

Article 179

(1) A person that has violated the secrecy of communications handled by a telecommunications carrier (including a communication mentioned in Article 164, paragraph (3), a notice under Article 116-2, paragraph (2), item (i), subitem (b), made by an approved association for tackling transmission-type cyberattacks to telecommunications facilities, which is deemed by paragraphs

---

7 Act of No. 151 of 2002.

8 Act No. 86 of 1964.

(4) and (5) of the same article to be a communication pertaining to the handling by a telecommunications carrier, and an electronic or magnetic record of a communications history under subitem (b) of item (ii) of the same paragraph handled by an approved association for tackling transmission-type cyberattacks to telecommunications facilities) is punished by not more than two years or a fine of not more than one million yen.

(2) A person engaging in telecommunications business (including those engaged in the business set forth in item (i) or item (ii) of paragraph (2) of Article 116-2, to be carried out by an approved association for tackling transmission-type cyberattacks to telecommunications facilities, which is deemed by paragraphs (4) and (5) of Article 164) that has undertaken the act set forth in the preceding paragraph is punished by imprisonment of not more than three years or a fine of not more than two million yen.

(3) [Omitted]

(viii) Penal Code[9] (→ IV, VI)

Article 35 (Justifiable Acts)

An act performed in accordance with laws and regulations or in the pursuit of lawful business is not punishable.

Article 37 (Aversion of Present Danger)

(1) An act unavoidably performed to avert a present danger to the life, body, liberty or property of oneself or any other person is not punishable only when the harm produced by that act does not exceed the harm to be averted; provided, however, that an act causing excessive harm may lead to the punishment being reduced or may exculpate the offender in light of the circumstances.

(2) The preceding paragraph does not apply to a person under special professional obligation.

(ix) Personal Information Protection Guidelines for Telecommunications Businesses[10] (→ IV)

Article 15 (Restriction on Third Party Provision)

(1) No telecommunications carrier may provide personal data to a third party, without obtaining the principal's prior consent, except in those cases set forth in the following items:

(i) cases based on laws and regulations;

(ii)~(iv) [Omitted]

(2)~(11) [Omitted]

9 Act No. 45 of 1907.

10 Public Notice No. 152 of April 18, 2017 of the Ministry of Internal Affairs and Communicatio ns.

(x) Act on the Protection of Personal Information[11] (→ II, IV, VI)

Article 2 (Definitions)

(1) The term "personal information" as used in this Act means information relating to a living individual that falls under any one of the following items:

(i)~(ii) [Omitted]

(2)~(7) [Omitted]

(8) The term "principal" as used in this Act means a specific individual identifiable by personal information.

(9)~(10) [Omitted]

Article 23 (Restriction on Third Party Provision)

(1) A personal information handling business operator will not provide personal data to a third party, without obtaining the principal's prior consent, except in those cases set forth in the following items:

(i) cases based on laws and regulations;

(ii)~(iii) [Omitted]

(iv) cases in which there is a need to cooperate with a central government organization or a local government, or a person entrusted by them in performing affairs prescribed by laws and regulations, and when there is a possibility that obtaining the principal's consent would interfere with the performance of the said affairs.

(2)~(6) [Omitted]

(xi) Act on the Protection of Personal Information Held on Administrative Organs[12] (→ IV)

Article 12 (Right to Request Disclosure)

(1) Any person may, pursuant to the provisions of this Act, request that the head of an administrative organ disclose retained personal information which the administrative organ holds on that person.

(2) [Omitted]

Article 27 (Right to Request Corrections)

(1) Any person who thinks that the content of retained personal information (limited to those listed in the following items; the same applies in Article 36, paragraph (1)) for which that person is the principal is untrue may, pursuant to the provisions of this Act, make a request for correction (including addition or deletion; the same applies hereinafter) of the retained personal information to the head of the administrative organ holding the retained personal information; provided, however, that this does not apply if a special procedure for correction of the retained personal information is prescribed by another law or an order based on another law:

(i)~(iii) [Omitted]

---

11 Act No. 57 of 2003.

12 Act No. 58 of 2003.

(2)~(3) [Omitted]

Article 36 (Right to Request Suspension of Use)

(1) Any person who thinks that retained personal information for which that person is the principal falls under any of the following items may, pursuant to the provisions of this Act, make a request for the measures specified in the respective items to the head of the administrative organ holding the retained personal information; provided, however, that this does not apply if a special procedure for suspension of use, deletion, or suspension of provision (hereinafter referred to as "suspension of use") of the retained personal information is prescribed by another law or an order based on another law:

(i)~(ii) [Omitted]

(2)~(3) [Omitted]

Article 45 (Exclusion from Application)

(1) The provisions of Chapter IV do not apply to retained personal information relating to a judgment in a criminal case or juvenile case, a disposition executed by a public prosecutor, public prosecutor's assistant officer, or judicial police official, execution of a punishment or protective measure, post-incarceration rehabilitation services, or pardon (limited to retained personal information relating to a person who received that judgment or measure, a person towards whom the punishment or protective measure was executed, a person who applied for post-incarceration rehabilitation services, or a person who filed a petition for pardon).

(2) [Omitted]

III. Other Foreign Laws

(i) The Constitution of the United States of America[13] (→ IV)

Amendment IV

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

(ii) U.S. Federal Rules of Criminal Procedure[14] (→ IV, V)

Rule 4.1. Complaint, Warrant, or Summons by Telephone or Other Reliable Electronic Means

Primary tabs

13 The Constitution of the United States of America, *available at* https://www.law.cornell.edu/constitution

14 Federal Rules of Criminal Procedure, *available at* https://www.law.cornell.edu/rules/frcrmp

(a) In General. A magistrate judge may consider information communicated by telephone or other reliable electronic means when reviewing a complaint or deciding whether to issue a warrant or summons.

(b) Procedures. If a magistrate judge decides to proceed under this rule, the following procedures apply:

(1) Taking Testimony Under Oath. The judge must place under oath — and may examine — the applicant and any person on whose testimony the application is based.

(2) Creating a Record of the Testimony and Exhibits.

(A)~(B) [Omitted]

(3) Preparing a Proposed Duplicate Original of a Complaint, Warrant, or Summons. The applicant must prepare a proposed duplicate original of a complaint, warrant, or summons, and must read or otherwise transmit its contents verbatim to the judge.

(4) Preparing an Original Complaint, Warrant, or Summons. If the applicant reads the contents of the proposed duplicate original, the judge must enter those contents into an original complaint, warrant, or summons. If the applicant transmits the contents by reliable electronic means, the transmission received by the judge may serve as the original.

(5) Modification. The judge may modify the complaint, warrant, or summons. The judge must then:

(A) transmit the modified version to the applicant by reliable electronic means; or

(B) file the modified original and direct the applicant to modify the proposed duplicate original accordingly.

(6) Issuance. To issue the warrant or summons, the judge must:

(A) sign the original documents;

(B) enter the date and time of issuance on the warrant or summons; and

(C) transmit the warrant or summons by reliable electronic means to the applicant or direct the applicant to sign the judge's name and enter the date and time on the duplicate original.

(c) Suppression Limited. Absent a finding of bad faith, evidence obtained from a warrant issued under this rule is not subject to suppression on the ground that issuing the warrant in this manner was unreasonable under the circumstances.

Rule 41. Search and Seizure

(a) Scope and Definitions.

(1) [Omitted]

(2) Definitions. The following definitions apply under this rule:

(A) "Property" includes documents, books, papers, any other tangible objects, and information.

(B)~(E) [Omitted]

(b) Venue for a Warrant Application. At the request of a federal law enforcement officer or an attorney for the government:

(1)~(5) [Omitted]

(6) a magistrate judge with authority in any district where activities related to a crime may have occurred has authority to issue a warrant to use remote access to search electronic storage

media and to seize or copy electronically stored information located within or outside that district if:

(A) the district where the media or information is located has been concealed through technological means; or

(B) in an investigation of a violation of 18 U.S.C. § 1030(a)(5), the media are protected computers that have been damaged without authorization and are located in five or more districts.

(c)~(f) [Omitted]

(iii) Stored Communications Act (SCA: provisions other than those amended by the CLOUD Act)[15] (→ IV)

18 U.S. Code § 2705. Delayed notice

(a) [Omitted]

(b) Preclusion of Notice to Subject of Governmental Access.—A governmental entity acting under section 2703, when it is not required to notify the subscriber or customer under section 2703(b)(1), or to the extent that it may delay such notice pursuant to subsection (a) of this section, may apply to a court for an order commanding a provider of electronic communications service or remote computing service to whom a warrant, subpoena, or court order is directed, for such period as the court deems appropriate, not to notify any other person of the existence of the warrant, subpoena, or court order. The court shall enter such an order if it determines that there is reason to believe that notification of the existence of the warrant, subpoena, or court order will result in—

(1) endangering the life or physical safety of an individual;

(2) flight from prosecution;

(3) destruction of or tampering with evidence;

(4) intimidation of potential witnesses; or

(5) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

(iv) The German Code of Criminal Procedure (English translation)[16] (→ IV)

Section 110 Examination of Papers

(1)~(2) [Omitted]

(3) The examination of an electronic storage medium at the premises of the person affected by the search may be extended to cover also physically separate storage media insofar as they are accessible from the storage medium if there is a concern that the data sought would otherwise be lost. Data which may be of significance for the investigation may be secured; Section 98 subsection (2) shall apply mutatis mutandis.

---

15 18 U.S. Code CHAPTER 121—STORED WIRE AND ELECTRONIC COMMUNICATIONS A ND TRANSACTIONAL RECORDS ACCESS, *available at* https://www.law.cornell.edu/uscode/text/18/part-I/chapter-121https://www.law.cornell.edu/uscode/text/18/part-I/chapter-121

16 THE GERMAN CODE OF CRIMINAL PROCEDURE, *available at* https://www.gesetze-im-internet.de/englisch_stpo/englisch_stpo.html

(v) U.K. Regulation of Investigatory Powers Act (RIPA)[17] (→ IV)

49 Notices requiring disclosure.

(1) This section applies where any protected information—

(a) has come into the possession of any person by means of the exercise of a statutory power to seize, detain, inspect, search or otherwise to interfere with documents or other property, or is likely to do so;

(b) has come into the possession of any person by means of the exercise of any statutory power to intercept communications or obtain secondary data from communications, or is likely to do so;

(c) has come into the possession of any person by means of the exercise of any power conferred by an authorisation under section 22(3) or (3B) or under Part II Part 3 of the Investigatory Powers Act 2016 or Part 2 of this Act, or as a result of the giving of a notice under section 22(4) in pursuance of an authorisation under Part 3 of the Act of 2016 or as the result of the issue of a warrant under Chapter 2 of Part 6 of the Act of 2016, or is likely to do so;

(d) has come into the possession of any person as a result of having been provided or disclosed in pursuance of any statutory duty (whether or not one arising as a result of a request for information), or is likely to do so; or

(e) has, by any other lawful means not involving the exercise of statutory powers, come into the possession of any of the intelligence services, the police, the National Crime Agency or Her Majesty's Revenue and Customs, or is likely so to come into the possession of any of those services, the police, the National Crime Agency or Her Majesty's Revenue and Customs.

(2) If any person with the appropriate permission under Schedule 2 believes, on reasonable grounds—

(a) that a key to the protected information is in the possession of any person,

(b) that the imposition of a disclosure requirement in respect of the protected information is—

(i) necessary on grounds falling within subsection (3), or

(ii) necessary for the purpose of securing the effective exercise or proper performance by any public authority of any statutory power or statutory duty,

(c) that the imposition of such a requirement is proportionate to what is sought to be achieved by its imposition, and

(d) that it is not reasonably practicable for the person with the appropriate permission to obtain possession of the protected information in an intelligible form without the giving of a notice under this section, the person with that permission may, by notice to the person whom he believes to have possession of the key, impose a disclosure requirement in respect of the protected information.

(3) A disclosure requirement in respect of any protected information is necessary on grounds falling within this subsection if it is necessary—

(a) in the interests of national security;

(b) for the purpose of preventing or detecting crime; or

(c) in the interests of the economic well-being of the United Kingdom.

---

[17] Regulation of Investigatory Powers Act 2000, *available at* http://www.legislation.gov.uk/ukpga/2000/23/contents

(4)~(11) [Omitted]

50 Effect of notice imposing disclosure requirement.

(1) Subject to the following provisions of this section, the effect of a section 49 notice imposing a disclosure requirement in respect of any protected information on a person who is in possession at a relevant time of both the protected information and a means of obtaining access to the information and of disclosing it in an intelligible form is that he—

(a) shall be entitled to use any key in his possession to obtain access to the information or to put it into an intelligible form; and

(b) shall be required, in accordance with the notice imposing the requirement, to make a disclosure of the information in an intelligible form.

(2)~(10) [Omitted]

(iv) Australian Telecommunications and Other Legislation Amendment (Assistance and Access) Bill [18](→ IV)

317B Definitions

electronic protection includes:

(a) authentication; and

(b) encryption.

317E Listed acts or things

(1) For the purposes of the application of this Part to a designated communications provider, listed act or thing means:

(a) removing one or more forms of electronic protection that are or were applied by, or on behalf of, the provider; or

(b) providing technical information; or

(c) installing, maintaining, testing or using software or equipment; or

(d) ensuring that information obtained in connection with the execution of a warrant or authorisation is given in a particular format; or

(da) an act or thing done to assist in, or facilitate:

(i) giving effect to a warrant or authorisation under a law of the Commonwealth, a State or a Territory; or

(ii) the effective receipt of information in connection with a warrant or authorisation under a law of the Commonwealth, a State or a Territory; or

(e) facilitating or assisting access to whichever of the following are the subject of eligible activities of the provider:

(i) a facility;

(ii) customer equipment;

---

[18] 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

(iii) a data processing device;

(iv) a listed carriage service;

(v) a service that facilitates, or is ancillary or incidental to, the supply of a listed carriage service;

(vi) an electronic service;

(vii) a service that facilitates, or is ancillary or incidental to, the provision of an electronic service;

(viii) software used, for use, or likely to be used, in connection with a listed carriage service;

(ix) software used, for use, or likely to be used, in connection with an electronic service;

(x) software that is capable of being installed on a computer, or other equipment, that is, or is likely to be, connected to a telecommunications network; or

(f) assisting with the testing, modification, development or maintenance of a technology or capability; or

(g) notifying particular kinds of changes to, or developments affecting, eligible activities of the designated communications provider, if the changes are relevant to the execution of a warrant or authorisation; or

(h) modifying, or facilitating the modification of, any of the characteristics of a service provided by the designated communications provider; or

(i) substituting, or facilitating the substitution of, a service provided by the designated communications provider for:

(i) another service provided by the provider; or

(ii) a service provided by another designated communications provider; or

(j) an act or thing done to conceal the fact that any thing has been done covertly in the performance of a function, or the exercise of a power, conferred by a law of the Commonwealth, a State or a Territory, so far as the function or power relates to:

(i) enforcing the criminal law, so far as it relates to serious Australian offences; or

(ii) assisting the enforcement of the criminal laws in force in a foreign country, so far as those laws relate to serious foreign offences; or

(iii) the interests of Australia's national security, the interests of Australia's foreign relations or the interests of Australia's national economic well-being.

317L Technical assistance notices

(1) The Director-General of Security or the chief officer of an interception agency may give a designated communications provider a notice, to be known as a technical assistance notice, that requires the provider to do one or more specified acts or things that:

(a) are in connection with any or all of the eligible activities of 34 the provider; and

(b) are covered by subsection (2).

Note: Section 317ZK deals with the terms and conditions on which such a 3 requirement is to be complied with.

(2) The specified acts or things must be by way of giving help to:

(a) in a case where the technical assistance notice is given by the Director-General of Security—ASIO; or

(b) in a case where the technical assistance notice is given by the chief officer of an interception agency—the agency;

in relation to:

(c) the performance of a function, or the exercise of a power, conferred by or under a law of the Commonwealth, a State or a Territory, so far as the function or power relates to:

(i) enforcing the criminal law, so far as it relates to serious Australian offences; or

(ii) assisting the enforcement of the criminal laws in force 16 in a foreign country, so far as those laws relate to serious foreign offences; or

(iii) safeguarding national security; or

(d) a matter that facilitates, or is ancillary or incidental to, a matter covered by paragraph (c).

(2A) The specified acts or things must not be directed towards ensuring that a designated communications provider is capable of giving help to ASIO or an interception agency.

Listed acts or things

(3) The acts or things specified in a technical assistance notice given to a designated communications provider must be listed acts or things, so long as those acts or things:

(a) are in connection with any or all of the eligible activities of the provider; and

(b) are covered by subsection (2).

Note: For listed acts or things, see section 317E.

(vii) EU General Data Protection Regulation (GDPR)[19] (→ V)

Article 4 Transfers or disclosures not authorised by Union law

Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to this Chapter.

IV. Treaties, Conventions, and Executive Agreements

(i) Agreement Between Japan and the United States of America Concerning Digital Trade[20] (→ V)

Article 21 Information and Communication Technology Goods that Use Cryptography

1~2. [Omitted]

3. With respect to an ICT good that uses cryptography and is designed for commercial applications, neither Party shall require a manufacturer or supplier of the ICT good, as a condition of the manufacture, sale, distribution, import, or use of the ICT good, to:

---

19 General Data Protection Regulation, *available at* https://gdpr-info.eu/

20 Agreement Between Japan And the United States of America Concerning Digital Trade, *availab le at* https://www.mofa.go.jp/mofaj/ila/et/page3_002912.html

(a) transfer or provide access to any proprietary information relating to cryptography, including by disclosing a particular technology or production process or other information, for example, a private key or other secret parameter, algorithm specification, or other design detail, to the Party or a person in the territory of the Party;

(b) partner or otherwise cooperate with a person in the territory of the Party in the development, manufacture, sale, distribution, import, or use of the ICT good; or

(c) use or integrate a particular cryptographic algorithm or cipher.

(ii) Convention on Cybercrime[21] (→ V)

Article 18 Production order

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:

a a person in its 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; and

b 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.

2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

3 For the purpose of this article, the term "subscriber information" 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 and by which can be established:

a the type of communication service used, the technical provisions taken thereto and the period of service;

b the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;

c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.

Article 32 Trans-border access to stored computer data with consent or where publicly available

A Party may, without the authorisation of another Party:

a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or

b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

[21] Convention on Cybercrime, *available at* https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

(iii) Treaty between Japan and the United States of America on Mutual Legal Assistance in Criminal Matters[22] (→ V)

Article 2

1. [Omitted]
2. Requests for assistance under this Treaty shall be made by the Central Authority of the requesting Party to the Central Authority of the requested Party.
3. The Central Authorities of the Contracting Parties shall communicate directly with one another for the purposes of this Treaty.

(iv) US-UK Executive Agreement (→ V, VI)[23]

Article 1: Definitions

For the purposes of this Agreement:

1~13. [Omitted]

14. Serious Crime means an offense that is punishable by a maximum term of imprisonment of at least three years.

15~16. [Omitted]

Article 2: Purpose of the Agreement

l. The purpose of this Agreement is to advance public safety and security, and to protect privacy, civil liberties, and an open Internet, by resolving potential conflicts of "legal obligations when communications service providers are served with Legal Process from one Party for the production or preservation of electronic data, where those providers may also be subject to the laws of the other Party. The Agreement provides an efficient, effective, data protection-compatible and privacy-protective means for each. Party to obtain, subject to appropriate targeting limitations, electronic data relating to the prevention, detection, investigation, or prosecution of Serious Crime, in a manner consistent with its law and the law of the other Party.

2~3. [Omitted]

Article 4: Targeting Restrictions

1~2. [Omitted]

---

22 Treaty between Japan and the United States of America on Mutual Legal Assistance in Criminal Matters, *available at* https://www.mofa.go.jp/mofaj/gaiko/treaty/treaty159_3.html

23 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, *available at* https://www.justice.gov/ag/page/file/1207496/download#Agreement%20between%20the%20Government%20of%20the%20United%20States%20of%20America%20and%20the%20Government%20of%20the%20United%20Kingdom%20of%20Great%20Britain%20and%20Northern%20Ireland%20on%20Access%20to%20Electronic%20Data%20for%20the%20Purpose%20of%20Countering%20Serious%20Crimes)

3. Orders subject to this Agreement may not intentionally target a Receiving-Party Person, and each Party shall adopt targeting procedures designed to implement this requirement as described in Article 7.1.

4~5. [Omitted]

Article 5: Issuance and Transmission of Orders

1. Orders subject to this Agreement shall be issued. in compliance with the domestic law of the Issuing Party, and shall be based on requirements for a reasonable justification based on articulable and credible facts, particularity, legality, and severity regarding the conduct under investigation.
2. Orders subject to this Agreement shall be subject to review or oversight under the domestic law of the Issuing Party by a court, judge, magistrate, or other independent authority prior to, or in proceedings regarding, enforcement of the Order.
3. Orders subject to this Agreement for the interception of wire or electronic communications, and any extensions thereof, shall be for a fixed, limited duration; may not last longer than is reasonably necessary to accomplish the approved purposes of the Order; and shall be issued only if the same information could riot reasonably be obtained by another less intrusive method.
4. The Issuing Party may not issue an Order subject to this Agreement at the request of or to obtain information to provide to the Receiving Party or a third-party government.
5. The Issuing Party may issue . Orders subject to this Agreement directly to a Covered Provider. Such Orders shall. be transmitted by the Issuing Party's Designated Authority. The Designated Authorities of the Parties may mutually agree that the functions each carries out under Articles 5.5 through and inclusive of 5.9, 6.1, and 6.2 may be performed by additional authorities in whole or in part. The Designated Authorities of the Parties may, by mutual agreement, prescribe rules and conditions for any such authorities.
6. Prior to transmission, the Issuing Party's Designated Authority shall review the Orders for compliance with this Agreement.
7. Each Order subject to this Agreement must include a written certification by the Issuing Party's Designated Authority that the Order is lawful and complies with the Agreement, including the Issuing Party's substantive standards for Orders subject to this Agreement.
8. The Issuing Party's Designated Authority shall notify the Covered Provider that it invokes this Agreement with respect to the Order.
9. The Issuing Party's Designated Authority shall notify the Covered Provider of a point of contact at the Issuing Party's Designated Authority who can provide information on legal or practical issues relating to the Order.
10. In cases where an Order subject to this Agreement is issued for data in respect of an individual who is reasonably believed to be located outside the territory of the Issuing Party and is not a national of the Issuing Party, the Issuing Party's Designated Authority shall notify the appropriate authorities in the third country where the person is located, except in cases where the Issuing Party considers that notification would be detrimental to operational or national security, impede the conduct of an investigation, or imperil human rights.
11. The Parties agree that a Covered Provider that receives an Order subject to this Agreement may raise specific objections when it has reasonable belief that the Agreement may not properly be invoked with regard to the Order. Such objections should generally be raised in the first instance to the. Issuing Party's Designated Authority and in a reasonable time after receiving the Order. Upon receipt of objections to an Order from a Covered Provider, the Issuing Party's Designated Authority shall respond to the objections. If the objections are not resolved, the Parties agree that the Covered Provider may raise the objections to the Receiving Party's Designated Authority. The

Parties' Designated Authorities may confer in an effort to resolve any such objections and may meet periodically and as necessary to discuss and address any issues raised under this Agreement.

12. If the Receiving Party's Designated Authority concludes that the Agreement may not properly be invoked with respect to any . Order, it shall notify the Issuing Party's Designated Authority and the relevant Covered Provider of that conclusion, and this Agreement shall not apply to that Order.

Article 8: Limitations on Use and Transfer

1~3. [Omitted]

4. Where an Issuing Party has received data pursuant to Legal Process from a Covered Provider, and

   a. the United Kingdom has declared that its essential interests may be implicated by the introduction of such data as evidence in the prosecution's case in the United States for an offense for which the death penalty is sought; or

   b. the United States has declared that its essential interests may be implicated by the introduction of such data as evidence in the prosecution's case in the United Kingdom in a manner that raises freedom of speech concerns for the United States;

   prior to use of the data in a manner that is or could be contrary to those essential interests, the Issuing Party shall, via the Receiving Party's Designated Authority, obtain permission to do so. The Receiving Party's Designated Authority may grant permission, subject to such conditions as it deems necessary, and if it does so, the Issuing Party may only introduce this data in compliance with those conditions. If the Receiving Party does not grant approval, the Issuing Party shall not use the data it has received pursuant to the Legal Process in that manner.

5. [Omitted]

End.