The Legitimacy of Cross-Border Searches Through the Internet for Criminal Investigations

Taro Komukai, Aimi Ozaki

The legitimacy of cross-border searches through the Internet for criminal investigations

Taro Komukai[1] and Aimi Ozaki[2]

[1] College of Risk Management, Nihon University, Tokyo, Japan
komukai.taro@nihon-u.ac.jp
[2] KDDI Research, Inc., Tokyo, Japan

Abstract. On the Internet, information is transmitted instantaneously across borders. Enormous volumes of information are collected and stored throughout the world. Information on the Internet can also be subject to criminal investigations. The increasing problem for criminal justice authorities is that the information they seek to access is often stored in other States and is, therefore, outside their jurisdiction. Exercising a state power over data stored inside another State's territory could be a violation of sovereignty.

Discussing cross-border data investigation needs to consider both the sovereignty of the State in which the data are stored and human rights of the investigation subject. These issues are closely related to each other and, thus, likely to be confused. Regarding data collection for investigatory purposes, if there is no infringement of the investigation subject's human rights, concerns are rarely raised regarding sovereignty infringement. However, the existence of two types of investigation subjects, data subjects and data controllers, complicates the issue.

This paper provides an approach to improve cross-border data investigations, with due consideration of human rights and international law, by analyzing current international discussions in this field.

Keywords: Criminal Investigation, Privacy, Personal Data, International Law, Sovereignty

1 Criminal Investigation into Data Stored in Other States

1.1 Necessity for Overseas Search

On the Internet, information is transmitted instantaneously across borders. Criminals naturally use e-mails and various other services on the Internet. Sensors installed in smartphones and various Internet of Things (IoT) technologies enable the collection and storage of enormous volumes of information. Information on the Internet can also be subject to criminal investigations. However, because information is often stored outside the State of the investigating authorities, it is increasingly necessary for them to access data stored in other States.

Server computers providing cloud services via the Internet are scattered throughout the world. The user is not usually aware of where their data are located. For criminal

justice authorities, being able to access computer data is often indispensable for a successful investigation. In the future, investigations into computer data will further increase. Criminals must not be allowed to evade justice by placing data in foreign servers.

Conversely, a state is traditionally limited to exercising power within its own territory. Thus, while criminal justice authorities can compel suspects and network service providers to cooperate with investigations inside their own territorial jurisdiction, they cannot forcibly access data in other States. It is not clear whether a criminal justice authority can access data abroad through the computers of investigation subjects in its own territory.

For law enforcement authorities' cross-border investigations, there are schemes for mutual legal assistance. However, especially in relation to cyberspace, many of the problems with mutual legal assistance have been widely recognized. In the United States, the scheme based on mutual legal assistance treaties (MLATs) [1] is deemed time-consuming and cumbersome; moreover, there are no formal tools for sourcing assistance in conducting law enforcement searches in countries that have not signed an MLAT. [2] The Council of Europe has been promoting mutual legal assistance based on the Cybercrime Convention. However, the Cybercrime Convention Committee admits that, in some situations, this does not provide a realistic means to obtain information through investigation assistance, since this can take from six to 24 months. [3] Criminal justice authorities are increasingly demanding the ability to directly access data stored abroad, especially in emergency situations. In some cases, they also find it difficult to identify which State has jurisdiction over the data.

1.2 Interest to be Protected

Sovereignty is guaranteed as a fundamental principle of international law [4]. It is also considered as "[i]ndependence in regard to a portion of the globe" giving "the right to exercise therein, to the exclusion of any other State, the function of a State." [5] If a State's criminal justice authority exercises state power over the people and organizations based in other States, this infringes sovereignty. [6] Thus, the acquisition of data using state power is not allowed where this would threaten the independence of the State where the data exists.

There is also the issue of the investigation subject's human rights. For example, the Fourth Amendment of the Constitution of the United States, Article 8 of the European Convention on Human Rights, and Article 35 of the Constitution of Japan all require due process of law and adherence to statutory procedures in criminal investigations with compulsory measures. In this regard, access to data is only proper when it satisfies the following requirements: 1) the criminal justice authority accesses the data in accordance with lawful legal procedure; and 2) the legal procedure does not violate higher-level norms, such as international law and the constitution of the investigating State.

1.3 Scenarios to be Discussed

Criminal justice authorities are not allowed to investigate people and organizations based in another State without the latter's consent or other specific allocation of authority under international law, since such investigations are considered as the conduct of state power. [7]

Conversely, in conducting investigations, criminal justice authorities are generally allowed to access data stored in other States that is publicly available via the Internet, since such data can be considered publicly available also in the authorities' own State. [6] The Council of Europe's Cybercrime Convention affirms this in Article 32, paragraph 1.

When a criminal justice authority conducts a compulsory investigation of a computer in its own State, it faces the dilemma of whether it can order the submission of data in other States that are available through that computer. They have to consider both the sovereignty of the State where the data are stored and the investigation subjects' human rights. Investigation subjects include not only suspects or other related people, data subjects, but also data controllers such as internet service providers (ISPs), cloud service providers, etc. Data subjects are the people identified by the data, while data controllers are the people or organizations that determine the purpose and means of processing personal data. [8]

For situations in which criminal justice authorities directly contact private foreign service providers to request the voluntary provision of extraterritorial data, there are two principal conflicting views:

- Since the information that the service provider holds is not publicly available, gaining access to it requires either a specific allocation of authority under international law or the consent of the State enjoying enforcement jurisdiction over the data sought.
- A mere State request made directly to a private entity and unaccompanied by compulsion to comply does not interfere with the exclusive right of the other State to exercise enforcement jurisdiction within its territory. [6]

Regarding this issue, the Cybercrime Convention Committee proposes an international agreement to clarify in which cases direct cooperation may be obtained regardless of mutual legal assistance.

Based on the above, the scenarios in which criminal justice authorities face problems in accessing data stored in other States are summarized in Table 1.

Table 1. Problems in each scenario

Interest to be protected / Type of investigation	Sovereignty	Rights of Data Subject	Rights of Data Controller
Compulsory investigations of data subjects	Infringement of target state's sovereignty	Search or seizure without due process of law	No infringement of any interest
Compulsory investigations of data controllers	Infringement of target state's sovereignty	Search or seizure without due process of law	Search or seizure without due process of law
Request for cooperation to data controllers	Controversial	Invasion of privacy and data protection	No infringement of any interest

2 Cases

2.1 Microsoft Corp. v. United States, 829 F.3d 197 (2016)

The United States Department of Justice suspected that a mail account of the Web e-mail service provided by Microsoft was being used to promote the drug trade. Therefore, through a search and seizure warrant under the Stored Communications Act (SCA: 18 U.S.C. §§2701-2712 (2012)), the Department of Justice requested to Microsoft to disclose information relating to the mail account. Microsoft disclosed all the target information stored in the U.S. but refused to disclose information stored in a data center in Dublin, Ireland, in relation to which it filed a motion to quash.

The District Court dismissed Microsoft's motion, and imposed a civil contempt order against Microsoft for failing to comply with the warrant. On Microsoft's appeal, the Second Circuit Court reversed the District Court's denial of the motion to quash, vacated the order holding Microsoft in civil contempt, and remanded the matter to the District Court.

In upholding the Microsoft's appeal, the Second Circuit Court ruled that the SCA warrant is effective only within the U.S. The court explained that congressional legislation is assumed to apply only within the territorial jurisdiction of the U.S. unless a contrary intent is clearly shown with an affirmative indication; the SCA's provisions contain no such indication. The court also mentioned that the SCA and the warrant rule in the Federal Rules of Criminal Procedure should be interpreted to reflect their original purposes of protecting privacy.

The execution of the warrant was then determined by the Second Circuit Court to be extraterritorial law enforcement, because privacy was infringed in the location from

which the data were to be obtained. This case has now reached the U.S. Supreme Court, whose decision is expected in early 2018.

2.2 In re Search Warrant 232 F.Supp.3d 708

Prior to the Second Circuit Court's decision in the Microsoft case, Google's policy was to disclose information about customers' communication content stored in foreign countries in response to SCA warrants from criminal justice authorities.

However, after that decision, Google decided to reject SCA warrant requests for disclosure of information located in foreign countries. Consequently, the FBI sued Google to seek disclosure of such information. The United States District Court for Eastern District of Pennsylvania reaffirmed that SCA warrants are only effective within the United States. However, the court decided that the FBI could use the warrant to order Google to transfer information from a foreign server to Google's server in California, which would then become disclosable. The court reasoned that this transfer would not infringe any access or possessory interest of the customer, so it could not be considered as "seizure" to request the transfer of information for disclosure.

2.3 Unpublished Judgment of Tokyo Koto Saibansho [Tokyo High. Court], December 7, 2016 (Japan)

Through a revision to the Criminal Procedure Act in 2011 (Article 218, paragraph 2), Japan introduced a procedure to seize electronic data on the server to which a seized computer is connected via the Internet. In this case, having seized the suspect's PC under a warrant, the police obtained data from a Gmail account used by the suspect. As the Gmail mail server appeared to be located outside Japan, it was questioned whether the police could legally access the mail server.

The Yokohama District Court expressed concern that investigating information stored on a server in another State could be a violation of sovereignty. Given the high possibility that the server was located in a foreign country, and the law enforcement agency's awareness of this, the court held that the agency should not have accessed the Gmail data (Yokohama Chiho Saibansho [Yokohama Dist. Ct.], March 17, 2016, LEX/DB25542385 (Japan)).

The Tokyo High Court upheld the decision and ruled that the law enforcement agency should have conducted mutual legal assistance because the server was most likely located in a foreign country.

3 Discussion

3.1 Sovereignty

The U.S. courts act on the assumption that laws established in the U.S. can only be applied within the State's territorial jurisdiction. [9] U.S. law could only apply to a foreign jurisdiction when the U.S. Congress has clearly demonstrated such intention. It

thus appears that U.S. laws are established with consideration for other States' sovereignty, though Congress reserves the right to enact laws with extraterritorial application. It also seems permissible for criminal justice authorities to order people or entities within the territorial jurisdiction of the U.S. to disclose information stored in foreign States, pursuant to a lawful subpoena. [2] The rationale may be that this compulsory investigation concerns people or entities within the United States' territorial jurisdiction, rather than the information itself.

Academic discussions on this issue in the U.S. offer conflicting views. Jack L. Goldsmith insists that "territorial sovereignty" is a concept without clear definition and has never had definitive content; instead, it changes "in response to changed international circumstances, including changed technological circumstances." Goldsmith argues that "such searches are not prohibited by norms of territorial sovereignty, and are not without precedent." [10] Conversely, Patricia L. Bellia insists that although the searching State may view its actions as "merely advancing a claimed power to regulate extraterritorial conduct causing harmful effects within its own borders," the target State "may view a remote cross-border search itself as extra-territorial, conduct with harmful local effects." [11] Recently, two opposing views have been raised: the first contends that accessing data held overseas does not infringe the sovereignty of other States provided the Fourth Amendment is properly respected, [12] whereas the second insists that the Fourth Amendment should limit the government's authority, necessitating a new international framework that considers other States' sovereignty in determining the application of a U.S. warrant. [13] It is not disputed that the U.S. Congress can enact laws of extraterritorial application by clearly demonstrating this intention unless this draws international condemnation.

Conversely, Japanese courts deny criminal justice authorities the right to access data stored overseas, believing that, as an exercise of state power, this could constitute an infringement of another State's sovereignty. Japanese academics also suggest that data held overseas should only be accessed in accordance with Article 32 of the Cybercrime Convention: this requires a criminal justice authority to obtain lawful and voluntary consent from the State in which non-public data are stored [14] [15] [16].

However, Article 32 of the Cybercrime Convention was not intended to limit cross-border investigations only to the situation it details. The "Explanatory Report" of the Cybercrime Convention provides a detailed account of this article:

> The issue of when a Party is permitted to unilaterally access computer data stored in another Party without seeking mutual assistance was a question that the drafters of the Convention discussed at length. There was detailed consideration of instances in which it may be acceptable for States to act unilaterally and those in which it may not. The drafters ultimately determined that it was not yet possible to prepare a comprehensive, legally binding regime regulating this area. In part, this was due to a lack of concrete experience with such situations to date; and, in part, this was due to an understanding that the proper solution often turned on the precise circumstances of the individual case, thereby making it difficult to formulate general rules. Ultimately, the drafters decided to only set forth in Article 32 of the Convention situations in which all agreed that unilateral action is

> permissible. They agreed not to regulate other situations until such time as further experience has been gathered and further discussions may be held in light thereof. In this regard, Article 39, paragraph 3 provides that other situations are neither authorized, nor precluded. [17]

The Council of Europe's Cybercrime Convention Committee explored solutions for accessing evidence in the cloud for criminal justice purposes. They identified the necessity for criminal justice authorities to access overseas data without complying with Article 32, and found that this had already occurred. In particular, such a need arises where criminal justice authorities must preserve evidence, in cases of emergency, and, in some cases, where the authorities are empowered within their own State, subject to defined procedures and safeguards. The committee, therefore, recommended adding such a provision to the convention. [3]

In 2008, NATO established the Cooperative Cyber Defense Centre of Excellence. Its international group of experts conducted a scientific study on applying international law to cyber conflicts and cyberwar. Its second report, called "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations," was published in 2017. It proposed the following rule for extraterritorial law enforcement by a State:

> Rule 11-Extraterritorial enforcement jurisdiction
> A State may only exercise extraterritorial enforcement jurisdiction in relation to persons, objects, and cyber activities on the basis of:
> (a) a specific allocation of authority under international law; or
> (b) valid consent by a foreign government to exercise jurisdiction on its territory. [7]

In its explanation of this rule, Tallinn Manual 2.0 indicates that a criminal justice authority is allowed to exercise jurisdiction over an entity domiciled in its own State and require the entity to provide access to data stored in another State:

> Consider a situation involving a private entity domiciled in State A that stores its data in State B. State C, as part of its law enforcement activities wants to access that data. The Experts agreed that the consent of State A is insufficient to permit remote access by State C to the data in State B. Remotely accessing the data would be an exercise of enforcement jurisdiction by State C in State B that necessitates a specific allocation of authority under international law or State B's consent. However, the Experts likewise emphasized that State A may exercise its jurisdiction over the entity and, for example, require it to provide the respective data to State C. [6]

3.2 Rights of Investigation Subject

Investigation subjects' human rights must be protected in accordance with the due process of law guaranteed by each State's constitution. Human rights are also closely

connected to sovereignty infringement. When the human rights of people or entities in a given State's territory are infringed by another State, the independence of the former State is also often infringed. In fact, the U.S. courts consider infringement of the investigation subject's human rights when judging whether sovereignty has been infringed.

In the Microsoft case, the Second Circuit Court emphasized that the SCA is intended to protect users' right to privacy in the content of their communications; consequently, it considered that compulsory investigation of data held outside the jurisdiction of the U.S. infringed that right. Conversely, in the Google case, the District Court asserted that, with respect to human rights infringement, an order to transfer data from a foreign server to a computer in the U.S. does not differ form an order to transfer data from a server within the U.S. It should be noted that both these U.S. cases concerned the investigation of data controllers, rather than data subjects.

When a subject is directly investigated, they can refuse to provide the information and the criminal justice authority must comply with any applicable statutory procedure. PCs or other devices belonging to the suspect must not be compulsorily investigated without a warrant or subpoena limited in both subject and scope, and the suspect may lodge an objection against the warrant or subpoena. The right to privacy applies regardless of whether the data are stored in the investigating State or in another State.

On the contrary, when the investigation is conducted into data controllers, such as ISPs or cloud service providers, the data subject – whether a suspect or other relevant person – is not usually involved. Moreover, as a user of the network services, the data subject is often not even aware of what kind of data has been saved in computer servers. Consequently, information that users would not expect to be collected is stored without their awareness. Such an investigation could also be conducted without the awareness of the State in which the data are stored. [18]

The European Union adopted a directive on data protection associated with criminal investigation, prevention, etc., in 2016 (Directive (EU) 2016/680). Its preamble states:

> Where personal data move across borders it may put at increased risk the ability of natural persons to exercise data protection rights to protect themselves from the unlawful use or disclosure of those data. At the same time, supervisory authorities may find that they are unable to pursue complaints or conduct investigations relating to the activities outside their borders. Their efforts to work together in the cross-border context may also be hampered by insufficient preventative or remedial powers and inconsistent legal regimes. Therefore, there is a need to promote closer cooperation among data protection supervisory authorities to help them exchange information with their foreign counterparts. [19]

This means that natural persons, as data subjects, should be protected and that safeguards for data protection are also necessary in international cooperation between criminal justice authorities.

4 Conclusion

The need for investigation into computer data will continue to increase in the future. As the computers that provide networked services spread throughout the world, criminal justice authorities will increasingly need to investigate data stored in other States.

When a criminal justice authority directly investigates on the suspects or other related people, certain procedural guarantees apply regardless of whether the data is stored inside or outside the investigating State. Conversely, when an investigation targets a data controller, information that users do not expect to have been collected may be disclosed. This may pose more serious problems with respect to the data subject's data protection and privacy and the sovereignty of the Stata in which the data are stored. In particular, when a criminal justice authority requests data controllers to provide information voluntarily, the data subject is not involved and both statutory procedures and territorial sovereignty may be ignored.

From the above, and to advance the upholding of law and order in the world, discussions of cross-border data investigations from the viewpoint of international law and human rights protection should be based on the following understanding:

1. Subject to compliance with statutory procedures in its own territory, a criminal justice authority should be allowed to investigate data stored in another State when accessed via the computers or other devices through which the data subject, such as the suspect or other related person, was accessing the data, without any specific allocation of authority under international law.

2. A criminal justice authority should not be allowed to investigate data stored in another States pursuant to an investigation into a data controller without the consent of the State where the data are stored or a new and specific allocation of authority under international law, including the requirement to provide ex-post notification to the sovereign State where the data are located.

This work was supported by JSPS KAKENHI Grant Number JP18K01393.

References

1. Mutual Legal Assistance Treaties (2013) 7 FAM § 962.1. http://fam.state.gov/FAM/07FAM/07FAM0960.html.
2. Microsoft, 829 F.3d 197 (2016).
3. Council of Europe Cybercrime Convention Committee (2016) Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY, 9, pp 44-46.
4. Jennings R, Watts A (1993), Oppenheim's International Law. 9th edn, 564.

5. United Nations (1928) Island of Palmas arbitral award, 838
6. Schmitt MN (2017) Tallinn Manual 2.0. Cambridge University Press, pp 66-71.
7. SS Lotus (Fr v Turk), 1927 PCIJ (ser A) No 10 (Sept 7), 18.
8. European Union (2016) Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.
9. Morrison v. National Australia Bank Ltd. 561 US 247 (2010).
10. Goldsmith JL (2001) The Internet and the Legitimacy of Remote Cross-Border Searches Frontiers of Jurisdiction. 2001 U Chi Legal F 103: 109–117.
11. Bellia PL (2001) Chasing Bits across Borders. 2001 U Chi Legal F: 35, 42.
12. Kerr OS (2015) The Fourth Amendment and the Global Internet. Stan Law Rev 67: 285, 329.
13. Daskal J (2015) The Un-Territoriality of Data. Yale LJ 125: 326, 332-334.
14. Sugiyama T, Yoshida M (2012) An explanatory note about the revision of Penal code and Criminal Procedure Act to cope with the development of information processing. Hoso-Jiho 64(4): 101.
15. Yasutomi K (2017) Criminal Procedure Act, Sanseido. 2nd edn., 218.
16. Taguchi M (2017) Criminal Procedure Act, Koubindou. 7th edn., 119
17. Council of Europe (2001), Convention on Cybercrime - Explanatory Report - [2001] COETSER 8.
18. Komukai T (2018), Legal issues on Criminal Justice Access to data in the Cloud. ISPJ SIG Technical Report Vol.2018-EIP-79 No.6: 5.
19. European Union (2016) Directive 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.