Privacy Protection During Criminal Investigations of Personal Data Held by Third Parties

Taro Komukai

Privacy Protection during Criminal Investigations of Personal Data Held by Third Parties

Taro Komukai[1]

[1] Faculty of Global Informatics, Chuo University, Tokyo, Japan
komukai@tamacc.chuo-u.ac.jp

Abstract. This study focuses on privacy issues concerning personal data held by third parties during criminal investigations. The development of information technology has made it possible to collect and store vast amounts of information. Since data held by third parties are often provided to investigating authorities without the data subject's knowledge, serious privacy issues are a concern. There are two possible approaches to protecting the rights of the individual in such a situation. One relates to the restriction of investigating authorities and the other concerns the confidentiality obligations of data controllers. This study compares the relevant legislation on the privacy of personal data held by third parties and criminal investigations in the United States, the European Union, and Japan to propose appropriate solutions to address data privacy concerns. Specifically, the main recommendations of this study are that investigating authorities should be subject to certain restrictions and greater transparency requirements when processing personal data and that data controllers should be subject to greater confidentiality obligations.

Keywords: Criminal Investigation, Privacy, Data Protection, Due Process, Third Party Doctrine

1 Criminal Investigations of Data

1.1 Investigations of Third Parties

At present, various data on people are collected via networks and processed by computer systems, even more so now with the development of the Internet of Things. This information is stored and processed by big data and AI technologies, which continuously generates new data [1]. The use of data is expected to grow exponentially in the future [2].

The growth in data use has resulted in the accumulation of vast amounts of personal data to which investigating authorities have access [3]. When a crime is committed, investigating authorities use a variety of methods to look for clues and gather information on people they believe to be connected to the crime. Some of these data are generated using new technologies. For example, it is now a widespread practice to review CCTV footage and dashboard cameras for criminal investigations. In addition, many tracers are stored in information systems such as emails, social network messages, web services, shopping histories, location data, and access logs. It is very useful for investigators to collate this information to create lists of likely offenders, examine their behavioural history, and track down suspects [4]. The use of information

to improve the sophistication and efficiency of criminal investigations is desirable for society. However, as an increasing amount of information is collected in a variety of fields and its content is becoming increasingly diverse, new problems are arising because those who have an interest in the information and those who hold it do not always coincide [5].

If an investigating authority requests a person to provide their information, they can decide whether to accept or refuse the request after considering the implications. If the person refuses to cooperate with the investigation, the investigating authorities may still carry out the search with a warrant if they consider the information as necessary for the investigation. In this case, the investigating authority must present the warrant to the concerned person. This presentation enables the person to know the extent of the search to be carried out. If the person considers the procedure or scope of the search as inappropriate, they can lodge an objection with a court. The court will then re-examine whether the warrant is appropriate based on the person's arguments.

By contrast, if a third party such as a service provider is asked to provide data, protecting the privacy of the data subject is not necessarily important for this third party. The third-party data controller may voluntarily comply with a request from the investigating authority as long as they are not exposed to any legal liability. In this case, the fact that this data controller has provided information to the investigating authorities will not, in principle, be communicated to the data subject. They will only learn that the investigating authority has such information after it has been presented as evidence in court, and even then it may not be clear by what means the investigating authority has obtained the information (see Fig. 1).

If this third party refuses the request for cooperation, the investigating authorities may still conduct the search with a warrant. In this case, the search warrant is presented to the data controller and not to the data subject. Therefore, the data subject cannot object to this compulsory search when it takes place. In this case too, they can only raise their objections after the data have been submitted as evidence in court.

While there are different views and debates on how the right to privacy should be defined, it is widely agreed that there are cases where a person can object to state forces accessing their information on the basis of their right to privacy [6]. The question here is whether the rights of the individual are sufficiently protected during investigations of this nature into data held by third parties. There are two possible approaches to protecting the rights of the individual:

(i) Restrictions on the investigating authorities
(ii) Confidentiality obligations of the data controllers

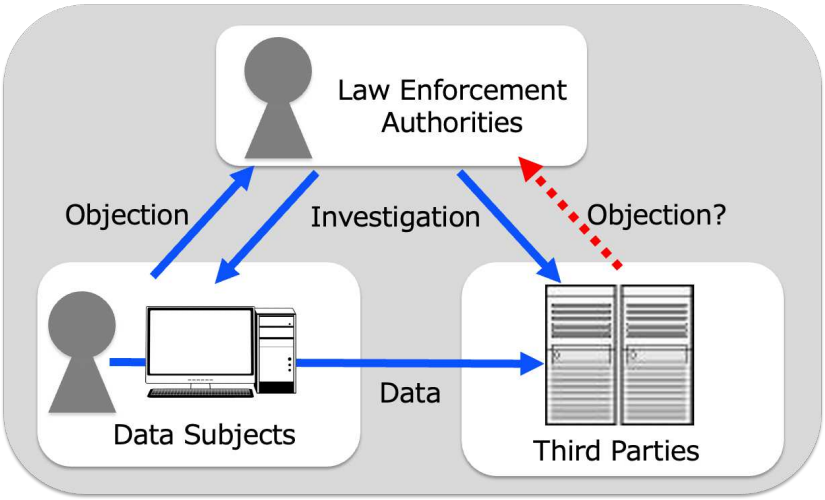

Fig. 1. Privacy problems in investigations of third-party records.

1.2 Restrictions on Investigating Authorities

When there is a concern that a search carried out by the investigating authority may be infringing on fundamental human rights, the authority must generally follow the statutory procedure. Arrests and seizures are typical violations of human rights, and such compulsory searches should, in principle, be carried out by the investigating authorities with a warrant issued by a judge in accordance with the law. The process and warrant principle is enshrined in the Fourth Amendment to the US Constitution, Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms, and Article 35 of the Japanese Constitution as essential to the protection of fundamental human rights.

Regarding searches on data held by third parties, the first question is whether an investigating authority may request data from a third party without a warrant. A warrant is required for a compulsory search because it restricts fundamental human rights, whereas a search can be carried out without a warrant if it does not infringe on fundamental human rights. Therefore, the question is whether the request for cooperation from a third party infringes on the fundamental human rights of the person concerned. Even if the investigating authority obtains personal data from a third party with a warrant, the warrant will only be presented to the third-party data controller. The question then arises whether fundamental human rights can be said to be protected when the data subject is not informed about the warrant.

1.3 Confidentiality Obligations of Data Controllers

If the investigating authority asks the data controller to cooperate in an investigation on a voluntary basis, it is the data controller who decides whether to cooperate. If the data controller is legally obliged to maintain confidentiality or there is a risk that the data

controller may be sued by the data subject for damages on the grounds of invasion of privacy, then the data controller will exercise caution. However, if the likelihood of such liability is low, it is not surprising that the data controller will cooperate with the investigating authorities. Therefore, it is important to know the confidentiality obligations of data controllers.

The rapidly growing importance of personal data for the right to privacy has led to the introduction of data protection legislation in many countries over the past few decades [7]. Personal data protection schemes often require data controllers to clarify the purposes for which personal data will be used to ensure transparency of processing. However, the provision of information to investigating authorities for criminal investigations is often permissible to comply with a legal obligation.

Special confidentiality obligations are imposed on those who handle personal data that are particularly sensitive and require strict protection. In some sectors such as telecommunications and medical services, there is a statutory obligation of confidentiality regarding the sensitive information handled during business, the breach of which is subject to sanctions. However, cooperation with investigating authorities is often an acceptable exception to such confidentiality obligations.

In addition, a large amount of information about users is collected and used by various operators, including tech giants such as Alphabet, Amazon, Apple, Meta, and Microsoft. These operators are not always under a special obligation of confidentiality in general and do not have a strong incentive to refuse requests from the investigating authorities from a legal perspective.

2 Comparison of Legal Systems

2.1 United States

Restrictions on Investigating Authorities. In the United States, fundamental human rights in criminal investigations are protected by the Fourth Amendment of the US Constitution [8]. The Fourth Amendment prohibits unreasonable searches and seizures and states the requirements for the issuance of a warrant. However, it does not say anything about when a warrant is required.

It is not assumed that a warrant is required for every collection of information conducted by an investigating authority and there is disagreement as to what types of searches require warrants [9]. A significant number of warrantless searches are conducted as ‘consent searches’. In some cases, a search may be permitted based on the consent of a third party who has actual control over the object to be searched such as a joint owner of the premise [10].

On the question of when a warrant is required, it was initially thought that intrusions into ‘persons, houses, papers, and effects’ were problematic, and that a warrant was required for searches that threatened freedom of action and private property rights in particular [11]. However, the development of technology has made it possible to obtain information about the privacy of the subject without such intrusion. In the case of Katz v. US [12], the Supreme Court reversed a conviction based on the warrantless interception of a conversation by placing an electronic listening device outside the

telephone booth used by the suspect for the conversation, holding that the prior justification procedure at the heart of the Fourth Amendment was lacking. It held that intrusion was no longer determinative because the importance of physical invasion had relatively diminished such that investigators could intercept conversations without physically entering the home and that the Fourth Amendment protects a 'reasonable expectation of privacy'.

After Katz v. US, the idea that a reasonable expectation of privacy was protected by the Fourth Amendment was established. However, the Supreme Court has long applied the 'third party doctrine' in a variety of contexts, holding that individuals do not have a 'reasonable expectation of privacy' in information they 'voluntarily convey' to third parties [13].

In 2018, the Supreme Court ruled that cell site location records held by wireless carriers were protected by the Fourth Amendment [14]. The case involved a court order requiring a mobile phone operator to submit location information (base station information) to the investigating authority. The 'reasonable grounds' requirement for issuing a court order is less strict than the probable cause for issuing a warrant. The court has ruled that the location information must be based on a warrant before it can be filed, as it also protects reasonable expectations of privacy. However, this judgement does not deny the third-party doctrine itself. The court has emphasised that cell site location information is 'unique' in terms of its power to reveal an 'exhaustive chronicle' of a person's daily life and its intimate details, which is the reason for not being applicable to the third-party doctrine.

Investigating authorities can also access the data held by third parties based on a subpoena. The issuance of a subpoena does not require a 'probable cause', but rather a much more moderate 'reasonableness' and the procedure is very simple [15]. A grand jury subpoena, for example, can be drafted by the public prosecutors themselves for books, documents, materials, data, and other objects. It is even permissible to call for a subpoena to ensure that 'the law has not been violated' [16]. In addition, objections to subpoenas are rarely effective.

Furthermore, the principle of the exclusion of unlawful collection is not very effective in protecting privacy, as there are insufficient penalties for disregarding the Fourth Amendment [17]. This is because even if the information collected is excluded from evidence in a trial, the privacy of the subject has already been violated and the exclusion of such evidence often has no effect on the conclusion of the judgement.

Confidentiality Obligations of Data Controllers. The United States does not have a comprehensive data protection federal law such as the General Data Protection Regulation (GDPR) in the European Union [18]. There are various laws protecting personal data in different sectors, including individual industries and public authorities. However, in most cases, the provision of personal data to investigating authorities is permitted. For some special categories of data such as telecommunications, the law imposes a duty of confidentiality on the business and the provision of data to the investigating authorities is restricted.

The Stored Communications Act in the United States (SCA, 18 U.S.C. §§ 2701–2712) requires the investigating authority to make requests to telecommunications

operators providing public telecommunications services only in accordance with statutory procedures. The required procedure depends on the type of information being processed. To obtain content data such as unopened email messages, a search and seizure warrant is required if the data have been stored for less than 90 days, while a subpoena or judicial order is required if the storage period is longer or if the data have already been accessed. Subpoenas and judicial orders of this kind require notice to the user. However, such notice may be excluded or delayed if there is reason to believe that it will have an adverse effect.

With respect to no-content data, which include a user's name, address, telephone number, network address, contractual information, and payment information, the SCA holds that the government may access such information with a subpoena from an administrative agency or grand jury without any obligation to notify the user. Nonetheless, it states that investigating authorities must obtain a warrant or court order to access, for example, addresses sent by email or information about sites visited, without requiring notice to the user. Further, while the SCA requires the user to be notified in some proceedings, its provisions only cover providers of public telecoms services and not tech giants, which are major players in handling information stored on the Internet.

In areas other than telecommunications such as medical institutions, there is a duty to protect patient confidentiality. In a case where a patient was arrested after reporting to the police that a urine test carried out at a national hospital had tested positive for cocaine, the Supreme Court ruled that this constituted an unreasonable search without the patient's consent [19].

2.2 European Union

Restrictions on Investigating Authorities. Article 8 of the European Convention of Human Rights stipulates that '[e]veryone has the right to respect for his private and family life, his home and his correspondence' [20]. Legal procedures are required for investigations that may violate fundamental human rights in member countries of the Council of Europe.

The European Union also adopted the Law Enforcement Directive [DIRECTIVE (EU) 2016/68] [21] in 2016 regarding processing personal data by investigating authorities and others. The Directive is designed to protect human rights in relation to processing personal data by investigating authorities for the prevention, investigation, detection, and prosecution of criminal offences and execution of criminal penalties. It requires member states to establish a system requiring that personal data collected by investigating authorities be used for clearly specified purposes, be used only to the extent appropriate in relation to those purposes, and not be retained for longer than necessary. The data subject must be able to know which investigating authority is processing the information, what data they are processing, and under what authority they are processing the information (Articles 13 and 14). The investigating authorities must create records of data processing (Article 24). Establishing a supervisory authority for data processing in this area and granting appropriate powers are also required (Articles 45–49) [21].

Confidentiality of the Data Controller. In the European Union, data protection is guaranteed as a fundamental human right. Paragraph 2 of Article 8 of the Charter of Fundamental Rights of the European Union provides that personal data 'must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law' and that '[e]veryone has the right of access to data which has been collected concerning him or her, and the right to have it rectified' [22].

To achieve protection, the GDPR requires a lawful basis [Article 6(1)] for processing personal data in general. Providing information to investigating authorities may be justified as a 'legal obligation' with the provision that it is only recognized as a 'legal obligation' if it is based on the law of an EU member state. Although there are considerable differences between the national laws of member states, the specific procedures required of the investigating authorities must be based on clear and specific provisions of legal obligation [23].

If an investigating authority requests cooperation on a voluntary basis, rather than through such a mandatory procedure, the provision of the data could be justified if it was 'for the purposes of the legitimate interests'. For a data controller to provide data based on a 'purpose of the legitimate interests', they must assess whether the information is necessary for the investigation and whether the scope of the information provided is proportionate to the purpose of the investigation. They must then be convinced that the provision of the information is indeed for 'the purpose of the legitimate interests'.

In the case of information relating to telecommunications, the legislation in most member states provides enhanced protection for the subject of the investigation. For example, special warrants are required in cases where investigations are carried out with respect to the interception of communications or communication records.

2.3 Japan

Restrictions on Investigating Authorities. Article 35 of the Constitution of Japan provides that, except in the case of a legitimate arrest, '[t]he right of all persons to be secure in their homes, papers and effects against entries, searches and seizures shall not be impaired except upon warrant issued for adequate cause and particularly describing the place to be searched and things to be seized' [24]. Article 197 of the Code of Criminal Procedure stipulates that a 'compulsory search shall not be applied unless otherwise provided for in this Act'. Therefore, when the investigating authority imposes a compulsory search, it must do so based on a warrant or other statutory procedure.

The Japanese Supreme Court has ruled that a 'compulsory search' means not only 'the way involving the use of tangible force', but also 'the way which it would be inappropriate to tolerate in the absence of special ground rules, such as acts of suppressing the will of an individual and realizing the purpose of an investigation forcibly by imposing restrictions on their body, residence or property' [25]. Although some may view the acquisition of personal data against the will of the individual as a compulsory measure, a request by the investigating authority for information from a

third party is not generally considered as such a measure. Article 197(2) of the Code of Criminal Procedure states that '[p]ublic offices or public or private organizations may be asked to make a report on necessary particulars relating to the investigation' and investigating authorities may make 'written inquiries on investigative matters' (so-called 'enquiry sheets'). However, this is a voluntary request for cooperation and there is no penalty for refusing the request. Indeed, investigating authorities request companies to provide information such as customers' names, addresses, telephone numbers, their usage history of services, purchase history of products, usage history of points, and GPS location information obtained from online games only on a voluntary basis [26].

In Japanese criminal investigations, the principle of voluntary investigation has been adopted [27] based on the belief that a compulsory search that violates or restricts human rights should be avoided as much as possible. Based on this principle, the voluntary cooperation of citizens with the investigating authorities has been considered as desirable by the Japanese authorities. It is not considered as problematic, at least in Japan, for investigating authorities to ask organisations to provide information about their customers or for organisations to respond voluntarily unless the information includes the secrecy of communications. The courts have often found the provision of information to the investigating authorities to be appropriate [28]. Thus, the fear of being held liable for an invasion of privacy by the person concerned is little deterrent in such cases.

The Act on the Protection of Personal Information (APPI) in Japan was amended in May 2021 and enacted in April 2022, which subjected investigating authorities to the supervision of the Personal Information Protection Commission. However, there are many provisions where criminal investigations are exempted, such as the provision for the restriction of use (Article 69 of the amended Act) and provision for ensuring transparency (Article 74 of the amended Act).

Confidentiality Obligations of Data Controllers. In Japan, Article 27 of the APPI generally prohibits data controllers from providing personal data to third parties without prior consent from the data subject. However, in cases where the investigating authorities request the provision of such data for an investigation, it can be provided without the consent of the data subject since it is a 'case based on laws and regulations'. The voluntary provision of information, including in response to an enquiry sheet from the investigating authority, also falls under the category of 'cases based on laws and regulations'. As long as the procedure is carried out properly, no infringement of the APPI will be an issue [29].

Regarding the secrecy of communications, voluntary cooperation with the investigating authorities is strictly prohibited. Article 21(2) of the Constitution of Japan prohibits the violation of 'the secrecy of any means of communication'. The Telecommunications Business Act provides for the prohibition (Article 4) and punishment (Article 179) of violating the secrecy of communications handled by a telecommunications carrier. Communication secrets include traffic and content data. A warrant issued by a judge is required for the investigating authorities to obtain information under the category of the secrecy of communications handled by a

telecommunications carrier and a warrant is required for the investigating authority to obtain the location data held by a mobile phone operator [30]. The Ministry of Internal Affairs and Communications has supervisory authority over the secrecy of communications handled by telecommunications carriers and administrative sanctions may be imposed for infringing the secrecy of communications.

There are other areas in which legal obligations for confidentiality are imposed. For example, doctors and other medical staff are prohibited from divulging to third parties the confidential information that they have acquired during their profession and there are penalties for breaching this (e.g. Article 134 of the Penal Code provides a penalty for physicians, pharmacists, pharmaceuticals distributors, midwives, and so on when disclosing their patients' confidential information). However, it is generally accepted that there is no breach of duty for cooperating with voluntary investigations, as it is considered as a justifiable reason [31].

3 Discussion

3.1 Due Process and Data Protection

Regarding criminal investigations, the protection of fundamental human rights has been ensured by the guarantee of due process. There is a view that the warrant principle should be more strictly enforced to cope with the fact that new technological developments allow investigating authorities to collect large amounts of information [32]. It is true that if the investigating authorities require the submission of data, due process must be carried out. The courts must also check whether the human rights of the subject have been unjustifiably infringed by the investigation. However, a warrant is not required when the data controller under investigation cooperates with the investigating authorities voluntarily and the courts will only check such warrantless searches if evidence obtained in the search is presented during a trial and the defendant questions the legality of the evidence.

The development of information technology has made it possible to collect and store vast amounts of information and the individual's concern about information held by third parties is much greater than before. Personal data protection systems have evolved in response to these concerns. For this reason, data protection legislation provides rules for transparency and individual involvement.

However, other aspects of data protection legislation also cause friction with the traditional approach to criminal investigations. In the field of criminal investigation, the gradual collection of information is a basic procedure and the request for investigative cooperation from third parties in possession of information is an extension of traditional investigations such as stakeouts and interviews. It is difficult to align criminal investigation with the concept of personal data protection, which limits the scope of data use by clarifying the purpose of use in advance. Regarding transparency, it is also undesirable for suspects to know what information the investigating authorities have about them.

However, it is possible to limit the use of personal data to the purposes necessary for criminal investigations and increase transparency to the extent that this does not hinder

criminal investigations. The EU Law Enforcement Directive presupposes that the protection of personal data is limited for purposes such as criminal investigations and this difficulty has been considered during the development of the system. For example, it is assumed that the right to information and access may be restricted for reasons of investigative necessity or public safety.

It is not desirable for criminal investigations to be unduly curtailed and for public safety to be compromised. To strike a balance between the need for criminal investigations and fundamental human rights, it is desirable to establish rules for the proper handling of information to the extent that it does not interfere with law enforcement and to ensure a certain level of transparency.

3.2 Duty of the Confidentiality of the Data Controller

Companies are increasingly aware that they should protect their customers' privacy. Some of the largest companies have adopted a policy of only providing information to law enforcement agencies when they are legally obliged to do so. They also publish transparency reports on their cooperation with law enforcement agencies. However, in many regions outside the European Union, it is up to individual companies to decide whether to take such actions.

If the data controller is obliged to maintain the confidentiality of the information, they will carefully consider whether to provide it. If there is a risk of penalties or sanctions for providing information in response to a request from an investigating authority, they will be reluctant to submit to a voluntary investigation. They will also be cautious about cooperating in a voluntary investigation if they are likely to be sued for damages due to the invasion of the person's privacy.

However, there may be cases where it is reasonable and socially acceptable to provide information voluntarily in response to a request from an investigating authority. For example, the GDPR requires that processing personal data in general, including its provision to investigating authorities, is justified. Cooperation with voluntary investigations is only permitted if it falls under the purpose of legitimate interests. If information is to be provided under this provision, the data controller must assess the necessity and proportionality of the provision and decide that it is appropriate. This is an example of a rule that strikes a balance between the need for investigation and protection of the individual's human rights.

Apart from personal data in general, special confidentiality obligations are imposed on data controllers with respect to information requiring particularly strong confidentiality, such as confidential communications and medical information. Nonetheless, the voluntary provision of information to cooperate with the investigating authorities may be excluded from the confidentiality obligation. However, given the sensitive nature of this information, it is advisable for investigators to seek a warrant when obtaining it and the provision of such information should generally still be prohibited without a warrant or other due process.

3.3 Ensuring Effectiveness

As already noted, the court review process does not function adequately when the investigating authority collects information from a third-party data controller. The courts reviewing what information is being collected and stored by the investigating authority and whether it is necessary and appropriate to do so is also difficult. Further, the confidentiality obligations of data controllers require a supervisory body independent of the investigating authority. For example, if the investigating authority supervises breaches of confidentiality, it is not possible to prosecute and punish those who cooperate in providing information requested by the same investigating authority.

In the European Union, data protection supervisory authorities are expected to fulfil this role. In Japan, a warrant is strictly required for the submission of confidential communications to an investigating authority because the Ministry of Internal Affairs and Communications supervises telecommunications operators and regulates any infringements on the secrecy of communications, not the criminal investigating authorities.

4 Conclusion

In light of the foregoing, it is desirable that, in general, the following legislation be put in place in relation to criminal investigations concerning the personal data held by third parties:

(1) Restrictions to investigating authorities.

- The investigating authority should be obliged to ensure that their processing of personal data is appropriate for the purposes for which it is used and that there is a degree of transparency by allowing access to data protection authorities.
- The processing of personal data by investigating authorities should be supervised by a data protection authority which is independent of the investigating authority.

(2) Confidentiality obligations of data controllers

- Data controllers should be prohibited from providing personal data to investigating authorities unless they are under an enforceable legal obligation or consider it appropriate in terms of necessity and proportionality.
- Information requiring a particularly strong duty of confidentiality, such as confidential communications and medical-related information, should not be provided unless there is a warrant.
- The confidentiality obligations of data controllers should be regulated by a supervisory body independent of the investigating authorities.

Table 1 compares the current systems in the United States, the European Union, and Japan from these perspectives.

Table 1. Restriction on investigating authorities and data controllers.

	Investigating authorities		**Data controllers**	
	Restriction	Safeguard	Restriction	Safeguard
US	Due Process (Amendment 4)	Judge (warrant)	Confidentiality Obligation	Private Action
EU	Due Process (ECHR* 8) Data Protection	Judge (warrant) DPA**	Data Protection	DPA**
Japan	Due Process (Constitution 35) Data Protection	Judge (warrant) DPA**	Secrecy of Communications	MIC***

* European Convention of Human Rights
** Data Protection Authority
*** Ministry of Internal Affairs and Communications

In the United States, the courts must supervise whether investigating authorities are conducting proper investigations. However, as it is difficult for the courts to supervise the processing of data by investigating authorities, a data protection authority should supervise it. In addition, there is no independent supervisory body for the confidentiality obligations of data controllers. In the United States, data subjects sue data controllers for the breach of confidentiality and investigating authorities for the illegal collection of information more often than in other countries, but there must be a clear basis in law for the plaintiff's claims to be recognised. Therefore, the legal restrictions on investigating authorities and confidentiality obligations of data controllers should be strengthened.

The European Union has made the most progress on protecting data subjects in this area, both in terms of restrictions on investigating authorities and in terms of the confidentiality obligations of data controllers, which are supervised by independent data protection authorities. However, it is up to the systems of each member state to ensure that data protection agencies are adequately informed by investigating authorities. It is thus necessary to constantly check whether the regulations are being properly implemented.

In Japan, investigating authorities are also subject to supervision by the data protection authority under the recently amended law, although many provisions exempt investigating authorities from restrictions. This needs to be amended so that appropriate supervision can take place. In addition, the confidentiality obligations of data controllers are not sufficiently enforced, except for information containing the secrecy of communications. Therefore, the confidentiality obligations of data controllers need to be strengthened.

Further studies are necessary for to propose more specific law reform in each area and country.

Acknowledgements. This work was supported by JSPS KAKENHI (Grant Number JP18K01393).

References

1. Falcon Dos, A.: Cyber privacy: Who has your data and why you should care. BenBella Books, Dallas (2020).
2. Schneier, B.: Data and Goliath. Norton, New York (2015).
3. Cate, H., Dempsey J. eds.: Bulk collection. Oxford University Press, New York (2017).
4. Ferguson, A.: The rise of big data policing. New York University Press, New York (2017).
5. Komukai, T.: Access to personal data held by third parties by investigating authorities and protection of the individual. Journal of Information and Communications Policy 4(1), 63–80 (2020).
6. Solove, D.: Understanding privacy. Harvard University Press, Cambridge (2008).
7. Fuster, G.: The emergence of personal data protection as a fundamental right of the EU. Springer, Cham. (2014).
8. United States Senate Webpage, Constitution of the United States, https://www.senate.gov/civics/constitution_item/constitution.htm, last accessed 2022/1/30.
9. Davies, T.: Recovering the original Fourth Amendment. Michigan Law Review 98(3), 547 (1999).
10. Dressler, J., Michaels, A., Simmons, R.: Understanding criminal procedure. Carolina Academic Press, Durham (2017).
11. Boyd v. United States, 116 U.S. 616, 627 (1886), Olmstead v. United States, 277 U.S. 438, Goldman v. United States, 316 US 129, 134–136.
12. Katz v. US, 389 U.S. 347 (1967).
13. United States v Miller, 425 U.S. 435, 442 (1976).
14. Carpenter v. United States, 138 S. Ct. 2206, 2221 (2018).
15. Taslitz, A., Henderson, S.: Reforming the grand jury to protect privacy in third party records. American University Law Review 64, 195 (2014).
16. United States v Morton Salt Co, 338 U.S. 632, 643 (1950).
17. Michael, P.: Taking data. University of Chicago Law Review 86, 77–141 (2019).
18. 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, https://eur-lex.europa.eu/eli/reg/2016/679/oj, last accessed 2022/1/30.
19. Ferguson v. City of Charleston, 532 U.S. 67 (2001).
20. Council of Europe, European Convention on Human Rights and Fundamental Freedoms, https://www.echr.coe.int/Documents/Convention_ENG.pdf, last accessed 2022/1/30.
21. 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, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016L0680, last accessed 2022/1/30.
22. Charter of Fundamental Rights of the European Union, 7 December 2000, https://www.europarl.europa.eu/charter/pdf/text_en.pdf, last accessed 2022/1/30.
23. Voigt, P., von dem Bussche, A.: The EU General Data Protection Regulation (GDPR): A practical guide. Springer, Cham. (2017).

24. Prime Minister of Japan and His Cabinet webpage, The Constitution of Japan, https://japan.kantei.go.jp/constitution_and_government_of_japan/constitution_e.html, last accessed 2022/1/30.
25. Judgment of Supreme Court, March 16, Japan (1976), https://www.courts.go.jp/app/hanrei_en/detail?id=47, last accessed 2022/1/30.
26. Kyodo News: Denuded private life, Sekai No. 921, pp. 106–114 (2019).
27. The Code of Criminal Investigations, Rules of the National Public Safety Commission No. 2, Article 99 (1957).
28. Judgment of Nagoya District Court, July 16, 2004, Japan (2004), https://www.courts.go.jp/app/hanrei_jp/detail4?id=7540, last accessed 2022/1/30.
29. Uga, K.: A Commentary of the Act on the Protection of Personal Information (APPI), 6th edn, Yuhikaku, Tokyo (2018)
30. Ministry of Internal Affairs and Communications (MIC): Commentary for guidelines For Protection Of Personal Information In Telecommunications Business, MIC Notice No. 152 of 2017; Last Amendment: MIC Notice No. 297 of 2017, September 2017 (Updated in February 2021), https://www.soumu.go.jp/main_content/000744055.pdf, last accessed 2022/1/30.
31. Yonemura, S.: Lectures on medical law. Nippon Hyoron Sha, Tokyo (2016).
32. Gray, D.: The Fourth Amendment in an age of surveillance. Cambridge University Press, Cambridge (2017).