



3-31-2023

Pandemics and the Protection of Privacy and Personal Information: Issues concerning the Restriction on the Right to Privacy in Emergencies

Fumio Shimpo
Keio University, shimpo@sfc.keio.ac.jp

Follow this and additional works at: <https://gensoken.toyo.ac.jp/japanese-society-and-culture>



Part of the [Constitutional Law Commons](#), [Health Law and Policy Commons](#), and the [Social Welfare Law Commons](#)

Recommended Citation

Shimpo, Fumio (2023) "Pandemics and the Protection of Privacy and Personal Information: Issues concerning the Restriction on the Right to Privacy in Emergencies," *Japanese Society and Culture*: Vol. 5, Article 1.

Available at: <https://gensoken.toyo.ac.jp/japanese-society-and-culture/vol5/iss1/1>

This Article is brought to you for free and open access by Institute of Social Sciences. It has been accepted for inclusion in Japanese Society and Culture by an authorized editor of Institute of Social Sciences.

[Received 26 September 2022 / Revised 20 October 2022 / Accepted 25 November 2022]

Pandemics and the Protection of Privacy and Personal Information: Issues Concerning the Restriction on the Right to Privacy in Emergencies

Fumio Shimpo^{*}

Abstract

This article focuses on issues which need to be considered in aiming to ensure both the effectiveness of infectious disease control measures and the protection of the right to privacy from the following perspectives.

(1) Issues regarding the restriction of the right to privacy in emergency situations, including (i) the types of measures taken in emergency situations and issues with respect to the restriction of the right to privacy in emergency situations, (ii) the normalisation, constancy and fixation of exceptional measures in emergency situations, (iii) dual-use and use for purposes different from those originally intended, (iv) acquisition of secondary information and the emergence of unexpected situations (e.g. the applicability of “body temperature” to special care-required personal information and the acquisition of secondary information associated with the measurement of body temperature, and examples of mission creep); and (5) the need to respond to over-reaction without recognising the urgency of the situation.

(2) Issues concerning privacy in countermeasures against infectious diseases, including (i) the procedures for requesting and disclosing personal information and privacy, (ii) the obligation to cooperate in active epidemiological investigations of specific patients and others based on the amended Infectious Diseases Control Act and restrictions on the right to privacy, (iii) the applicability of personal information concerning the acceptance of tests and other examinations as special care-required personal information, and (iv) the need to respond to over-reaction without recognising the urgency of the situation. (ii) the necessity of the implementation of information security management measures in relation to infectious disease countermeasures.

(3) Issues concerning the use of technology for the purpose of countermeasures against infectious diseases and privacy, including (i) the use of GPS location information, (ii) considerations required to resolve concerns in the introduction and spread of contact confirmation applications, (iii) the acquisition of biometric information and the use of biometrics, and (iv) sewage epidemiological surveys and privacy (privacy of drainage).

Keywords: Pandemics, COVID-19, Privacy, Personal Information, Data Protection, Public Health

^{*} Keio University, Faculty of Policy Management, Professor

I. Issues Concerning the Restriction on the Right to Privacy in Emergencies¹

1. Measures and Types of Issues Concerning the Restriction on the Right to Privacy in Emergency Situations

To deal with emergencies associated with the global spread of the Novel Coronavirus Infections, (COVID-19), countries have been implementing various response measures under the broad head of 'states of emergency'. A state of emergency is a response to an emergency situation rather than to a normal situation. However, if a state of emergency is normalised and continues for a prolonged duration, there is an obvious risk that it will no longer be considered an emergency.

There are three views on the restriction to the right to privacy. One view believes that restrictions hold only for the duration of an emergency, and are thus temporary. Another view expresses concern that there is no turning back even on the restrictions imposed on the right to privacy after the emergency has been lifted. The third view is a mix of both expectation and disappointment vis-à-vis the protection of privacy after the convergence of the views that insist on the usefulness of surveillance measures to control the spread of infectious diseases in emergency situations.

Some examples of these views are as follows. While we are forced to adjust our expectations of privacy, this situation does not mean that the valuable right to privacy and private choice will be restricted in the long term or permanently, but would rather only be limited by emergency measures "Technology, once deployed, cannot be 'rolled back,' and it is likely that the repeated claims that contact-tracing apps and COVID-19-related surveillance measures are transient measures until the pandemic is contained, are illusory" (Hartzog, 2020).² There is a "ratchet effect," which involves the loss of control (EDPB,

¹ 'Emergency management', (Article 15, Paragraph 2 of the Cabinet Law) refers to 'dealing with an urgent situation which has caused or is likely to cause serious damage to the lives, bodies, or property of the people and preventing the occurrence of such a situation'. The terms 'emergency situation' and 'extra-ordinary situation' are used mainly for provisions pertaining to events involving natural disasters. The meaning of 'emergency as a legal term differs according to the difference between 'time' and 'occasion'. The term 'emergency-response situation' is also used. Some examples of an 'emergency' include the following: 'matters related to measures to prevent the outbreak and spread of infectious diseases and to provide medical care in emergencies, (including ensuring a communication system between the national government and local governments and between local governments)', as stipulated under Article 9, Paragraph 2, Item 11 of the Infectious Diseases Act; and matters pertaining to the prevention and spread of infectious diseases and measures for the provision of medical care (including ensuring a communication system between the national and local governments and among local governments) in times of emergency. An example of 'in the case of an emergency', is the technical standards governing the various Compressed Natural Gas Acts (Article 7-2-13) as prescribed by the General High Pressure Gas Safety Regulations, (Ministry of International Trade and Industry Ordinance No 53, 1966) and the Safety Regulations for Industrial Complexes, (Ministry of International Trade and Industry Ordinance No 88, 1986) based on the High Pressure Gas Control Act, (Act No 204, 1951);, where the 'dispenser' shall be installed in a location where it can be promptly operated in the case of an emergency. Examples of 'emergency situations' include 'emergency measures for new strains of Influenza, etc' as found under Article 2, Item 4 of the Act on Special Measures against New Strains of Influenza, etc. (Act No 31, 2012), and the 'Act on Securing the Peace and Independence of Japan and the Security of the State and People in Armed Attack Situations, etc and Situations of Existential Crisis', (Act No. 79, 2003), Article 21 states that 'emergency situations are those which have a serious impact on the safety of the country and its citizens other than armed attack situations, etc, and existential crisis situations.' Only the Law on Armed Attack Situations stipulates that an 'emergency response situation' is one in which an act of killing or injuring a large number of people by means equivalent to an armed attack has occurred, or a situation in which it is recognised that there is an imminent danger of such an act occurring. The Nuclear Emergency Guideline, which guides nuclear disaster counter-measures, was revised in February 2013 to distinguish between 'emergency situations' and 'Emergency Action Levels, (EAL)'. Emergency measures', (e.g., Article 109 of the Basic Act on Disaster Control Measures (Act, No. 223,1961)) are deployed to deal with 'emergency situations' and 'emergencies.

² From a governance perspective, some observers have pointed out that "unless infectious disease apps are used within an appropriate data governance framework, the use of these apps will set a precedent for the unrestricted and unregulated use of sensitive data to be shared" (Terada, 2020).

2020; Suda, 2021). “It is useful to use the three tools used to converge the Coronavirus Infections (self-quarantine, contact tracing, and flow models using statistical and anonymous information) as a means of surveillance by the government (Big Brother)?” (Xu 2020).

Measures taken in an emergency situation and issues surrounding the restriction on the right to privacy in an emergency should be examined, assuming that they will not be limited to emergency situations and temporary restrictions will continue even after the emergency is lifted. Therefore, I would like to discuss the issues that must be considered during emergencies even after the situation has been resolved.

Table 1: Issues Associated with Measures to Limit Privacy During Emergency Situations

1.	Normalization of exceptional responses to Emergencies<Fixation<Normalization
2.	Dual use or use for a different purpose than the originally intended one
3.	Acquisition of secondary information and emergence of unexpected situations (function and mission creep)

2. Normalization of Exceptional Responses to Emergencies

There are problems associated with the normalisation of exceptional responses to emergencies. Temporary exceptions to emergency situations become permanent when they are implemented regularly. This can lead to a situation wherein individuals’ awareness of privacy protection and social efforts to protect privacy are diluted, and appropriate and necessary privacy protection measures are no longer taken. Even if restricting individual rights and interests as an emergency measure to combat the spread of an infectious disease is necessary, it is alarming that such restrictions may become a new norm. In an era wherein new infectious diseases like COVID-19 have emerged, we must co-exist with them and must not be forced to indulge in restrictions based on public welfare and health, when the basic rights of individuals are restricted and their privacy is violated. It is necessary to prevent such situations from being “normalized” and ourselves from becoming numb to recognizing problematic situations.

In previous cases, when surveillance cameras were installed everywhere for crime prevention, there were few opportunities to dispute their installation and use. Although problems may be identified with respect to the proper and fair use of information acquired by cameras (e.g., face recognition and identification), we are no longer particularly conscious of the existence of these cameras in our daily lives.

Continuation of exceptional measures for infectious disease control includes cases in which contact confirmation and tracking applications introduced for the purpose of preventing the spread of infection are used even after the infection has been contained, or in which systems and new procedures established for the purpose of controlling COVID-19 in order to realize the holding of a large-scale international event continue to be implemented even after the event has been held. Although the response to new infectious diseases and viruses is expected to move in the direction of convergence with the development of vaccines and treatments, it is possible to continue to use the decisions and mechanisms relied on as countermeasures even after convergence. Measures to prevent the normalization of the situation, in which people are no longer able to recognize that they are in a unique environment, must be considered during normal times and not during emergencies alone.

3. Dual Use or Use for a Different Purpose than Originally Intended

Issues related to “dual use” (Kodama, 2017),³ such as the use of one technology for other purposes, or misuse or abuse for purposes other than the original one,⁴ include the use of a technology introduced to prevent the spread of infections for surveillance and purposes aside from infection control.

With regard to the private sector, there is a view pointing out the concerns and uncertainty regarding the use of the technology for purposes other than the original purpose by the provider of the platform for contact verification applications (Hartzog, 2020). One example is the “Trace Together” contact tracing app, which was introduced in Singapore in March 2020 to track the contacts of people who may have been exposed to the new coronavirus. The government announced that the data collected by the app will be provided to the Singapore Police Force for use in criminal investigations after the pandemic (Sato, 2021). A change in the purpose because of a change in policy, such as the use of information obtained through a contact tracing app to prevent the spread of infection for criminal investigations can force people to refrain from using the app and the original purpose may not be achieved.

4. Acquisition of Secondary Information and Emergence of Unexpected Situations (function and mission creep)

1) Problems related to the Acquisition of Secondary Information

Problems related to the acquisition of secondary information and the emergence of unexpected situations (function creep) are likely to figure in the use of personal biometric data. As an issue concerning the acquisition of secondary information, I focus on “temperature checks.” A temperature check is an essential measure to prevent infection on the basis of certain standards. It is also effective in preventing the spread of infectious diseases. Therefore, refusing to take temperature readings on the grounds of personal privacy may be considered socially unacceptable given the pandemic, partly because the specific risk of privacy violation associated with temperature readings is not obvious.

The following are some of the issues related to temperature monitoring and personal information and privacy: (1) If body temperature measurements are required every day, changes in the body’s condition may become apparent through numerical changes; (2) secondary information may be obtained through the accumulation of body temperature data (equilibrium temperature); and (3) temperature monitoring may be conducted continuously and in situations wherein an individual cannot refuse, such as at the workplace. Issue (1) is mainly a privacy issue. Continuous temperature monitoring may reveal private health information, such as menstruation, pregnancy, and menopause in women (Natta et al., 2020). However, from the perspective of privacy impact, it is assumed that the temperature is taken precisely enough to reveal such changes in body condition, and therefore it is not possible to confirm such detailed changes in the body for the purpose of general countermeasures against infectious diseases. Issue (2) is related to personal information protection. If the normal temperature is revealed through the accumulation of body temperature (equilibrium temperature), information on “race” (Matsuda et

³ Dual-use is defined as “science and technology that can be applied to both civilian and military development (military-civilian dual-use), or more broadly, knowledge and technology that was originally created for public welfare and benefit but has the potential for abuse and misuse (good and bad dual-use), and ambiguity of use.”

⁴ The original intent of the phrase “attack is the greatest form of defense” as taught in Sun Tzu’s *The Art of War* is not to base one’s thinking on offense, but on the principle of defense, and then to attack when one sees an opportunity. There is a concern that defensive measures may not only become offensive but also wind up being most offensive.

al., 1985), which falls under the category of personal information requiring consideration as secondary information, may be unintentionally obtained. Issue (3) involves both privacy and personal information. To prevent the spread of infection, tele-commuting is recommended to reduce contact between people, and the number of opportunities to go to work is decreasing. However, it is difficult to perform certain tasks while tele-commuting. Thus, some companies conduct daily temperature checks upon arrival at work to prevent cluster outbreaks and other infectious diseases at the workplace. In Japan, although there are guidelines for countermeasures against infectious diseases, such as the “Guidelines for Countermeasures against H1N1 Influenza and Other Influenza Affecting Businesses and Workplaces,” there are no specific standards in terms of personal privacy or employment-related procedures for conducting temperature checks in the workplace or other places where an individual may not refuse.

The US Equal Employment Opportunity Commission (EEOC, 2020) has published criteria for the revocation of employment because of the employers’ periodic measurement of the temperature of their employees and confirmation of COVID-19 infection in new hires. Another discussion has pointed out issues with respect to “biometric data acquisition and use in the workplace, use of biometric data in wellness programs, and biometric data acquired through wearable devices” (Brown, 2020). There are issues surrounding the handling of body temperature and other values⁵ obtained using healthcare applications in the workplace. From a technical point of view, the degree of influence on privacy depends on the accuracy of the “body temperature” to be measured⁶ owing to the difference between (1) the measurement of body temperature using a “Medical Thermometer” as defined in the Pharmaceutical Affairs Law (Law concerning the Quality, Efficacy and Safety of Drugs, Medical Devices, etc.), and (2) measurement using a “thermometer.”⁷ As many as 46 out of 100 travelers infected with COVID-19 have passed through quarantine without having their temperatures checked (Quilty et al., 2020).

2) Applicability of Body Temperature to Personal Information Requiring Consideration and Secondary Information Associated with the Measurement of Body Temperature

Body temperature is not personal information if it is only a numerical value and cannot be easily cross-checked with other information. It does not fall under the category of “personal information (including

⁵ Issues related to mental health apps that measure stress indices using heart rate variability (HRV) analysis, and the use of apps in psychiatric telemedicine (Richer, 2020) and issues related to the acquisition of health information by apps and legal challenges (Helm and Georgatos, 2014) are identified.

⁶ The difference between the measurement of body temperature using a medical and regular thermometer is that the former involves the measurement of body temperature (equilibrium temperature) and central (core) temperature using a thermometer (Order for the Enforcement of the Act on Quality, Efficacy and Safety of Drugs, Medical Devices, etc., Appended Table 1 (related to Article 1), No. 16) as specified by the Pharmaceutical Affairs Act. Temperature measurement by the latter means the detection of abnormal temperature using a thermometer (infrared thermography camera, thermo-camera, body temperature measuring gun or spot radiation thermometer, and other non-contact or radiation thermometers such as temperature detectors). They are used for temperature control in all aspects of air conditioning, home appliances, and office automation equipment, automobiles, factories, etc. In infectious disease control, they are used for thermography and fever detection in order to check people suspected of having a fever.

⁷ The accuracy of the radiometric measurement varies according to the part of the body measured by the radiometer (Aizawa et al., 2000). The results of a verification of whether the ocular surface temperature measured in a non-contact manner on the iris through a radiation thermometer, where perhaps the core temperature index was analyzed through thermograms around the eye area in a constantly neutral environment, suggest that the ocular surface temperature, which is measured in a non-contact fashion with a radiation thermometer at the iris, does not directly reflect the iris’ temperature but is more likely to be the corneal temperature without blood flow control and is unlikely to be a core temperature indicator.

information that can be easily collated with other information to identify a specific individual),” as defined under Article 2, Item 1 of the Personal Information Law. Even where body temperature is considered personal information, it may or may not fall under the category of personal information requiring consideration.⁸ Cases where the information is obtained as a result of medical examinations, etc., as stipulated under Article 2, Item 2 of the Enforcement Order for the Act on the Protection of Personal Information (Cabinet Order No 507 of 2003), fall under the category of personal information requiring consideration. This does not apply to “cases in which information concerning an individual’s health, such as height, weight, blood pressure, pulse, body temperature, etc., has been obtained through a method unrelated to the business of medical examinations, medical treatment, etc., or related work” (example on page 14 of the Guidelines for the Act on the Protection of Personal Information; General Provisions).

The procedures for acquiring (measuring) body temperature information may be divided into the following categories: (1) acquisition of body temperature information that falls under the category of personal information requiring consideration (requiring the consent of the individual according to Article 17, Paragraph 2 of the Personal Information Law); (2) acquisition of body temperature information that is not personal information requiring consideration (requiring no consent of the individual); and (3) reporting of body temperature and other health conditions based on laws and regulations (falling under the category of cases based on laws and regulations according to Article 17, Paragraph 2, Item 1 of the Personal Information Law and requiring no consent of the individual).

3) Example of “Mission Creep”

Function creep⁹ is the use of a product in a manner that was not initially expected or planned. Mission creep is the use of the material beyond the originally expected range. For example, AliPay’s (支付宝) “National Health Code Rating System” (全国版健康码) (Jao, 2020; Mozur et al., 2020), which determines and displays the risk of being infected with COVID-19 for the sake of contact tracing, is used by the government to check compliance with mandatory quarantine requirements and home isolation. There is a suggestion that this is mission creep (Cohen, 2020).

5. The Need to Respond to “Overreactions” that do not Recognize the Real Urgency of a Given Situation

It is necessary to deal with emergency situations where there is a dilemma of having to handle vital information even when it constitutes the disclosure of personal information. Most information handled in the medical field is highly sensitive and requires caution, and since the full enforcement of the Personal

⁸ Under the EU’s General Data Protection Regulation (GDPR), body temperature is included under health-related and sensitive data under Item 15 of Article 4, and Article 9, respectively. Thus, the GDPR does not distinguish between cases where body temperature falls under the category of personal information requiring consideration and where it does not, as is the case with Japan’s Personal Information Law. Temperature information, which is sensitive data under the GDPR, does not fall under the category of personal information requiring consideration under Japan’s Personal Information Protection Law (Mori, 2020). However, it appears that this point refers to body temperature taken at work, which is unrelated to medical examinations, etc., in the General Rules of the Personal Information Law Guidelines.

⁹ An example of a legal issue related to function creep is a case in which a service that is automatically authenticated by a facial recognition device unintentionally handles secondary information on race. When the data were checked, it was found that the error was caused by skin color. There are many cases where errors were caused in the development stages of face recognition devices by skin color. At the development stage of a facial recognition device, the device is supposed to be technologically neutral in relation to racial discrimination. However, by analyzing the cause of the unexpected error, it was found that the use of the device resulted in racial discrimination.

Information Protection Law in 2005, there have been many cases of overreaction that have lacked common sense because of a cautious but unrealistic compliance with the law. One of the reasons for these overreactions is that the privacy protection measures, such as not displaying the names of patients by number and not displaying the names of hospitalized patients on the doors to their rooms, are equated with the procedures for restricting the provision of “personal data” to third parties, which is searchable and systematic as stipulated in the Personal Information Protection Law. As a result, overreactions, such as not being able to respond to urgent inquiries from family members about patients transported because of accidents, have been a characteristic of efforts to protect personal information in the medical field.

Some argue that countermeasures against the spread of infectious diseases have been hindered by problems in the interpretation of the laws and regulations within the personal information protection system. Thus, the Personal Information Protection Commission (PPC) published “The Handling of Personal Data for the Purpose of Preventing the Spread of New Coronavirus Infections.”¹⁰ When we check these opinions, it seems that most of them are not the result of defects in the current legal system but due to problems in legal interpretation. It is important to correct misunderstandings and overreactions, and to prevent them from becoming the norm. It is necessary to consider the problems that arise when exceptional responses in emergency situations continue in normal situations.

II Issues related to Privacy and Infectious Disease Control

1. Personal Information Requests, Disclosure Procedures, and Privacy

In the case of countermeasures against the spread of COVID-19, the disclosure of personal information on a “positive patient” is considered an excessive disclosure of information and is not permissible (Yokota, 2020).¹¹ On the other hand, if a situation arises where it is necessary to fight an infectious disease that causes serious symptoms equivalent to those of a Class 1 Infectious Disease, would the disclosure of necessary information, including personal information, be an effective means of preventing the spread of infection? We are currently awaiting the results of epidemiological research on overseas cases in which efforts have been made to prevent the spread of infection through the use or disclosure of information, rather than through the protection of personal information and privacy, to determine the extent to which the disclosure of information on infected persons contributed to the prevention of the spread of COVID-19.

There have been complex consequences. For example, in South Korea the acquisition of detailed personal information through the highly effective Contact Confirmation Method mandated the disclosure of the travel routes of infected persons and self-isolators (Jung, 2020; Mainichi Shimbun, 2020; BBC, 2020). South Korea enacted the Act on the Prevention and Control of Infectious Diseases (Itakura, 2020; Fujiwara, 2020), which was revised in December 2015 in response to the outbreak of the Middle East Respiratory Syndrome (MERS). According to this law and its enforcement ordinance, when it is

¹⁰ That personal data may be handled without the consent of the individual as a special emergency measure to counter the spread of COVID-19 was not indicated. To clarify that the views expressed by the PPC and the Ministry of Health, Labour, and Welfare are neither a special exception nor an emergency response for the purpose of combating the spread of COVID-19, the PPC published the “Handling of Personal Data for the Purpose of Preventing the Spread of the New Coronavirus Infection” https://www.ppc.go.jp/files/pdf/200402_1.pdf and answers to frequently asked questions on the Personal Information Protection Law Consultation Dial (attached) https://www.ppc.go.jp/files/pdf/200402_2.pdf.

¹¹ Germany’s legal response, which requires the provision of information related to infection prevention, is based on crisis communication principles.

necessary to prevent or deter the spread of infectious diseases, the procedures that can be implemented are legally stipulated, such as requesting and confirming the personal information of those who are positive or suspected positive (Article 76-2) and disclosing information during an infectious disease crisis (Article 34-2). The information that may be obtained based on this law includes: “1. personal information such as family name, resident registration number, address and telephone number (including cell phone number); 2. prescriptions and medical records; 3. immigration records for the period of time specified by the Minister of Health and Welfare; 4. other information specified by Presidential Ordinance to ascertain the various movements of the individual. Article 32-2 of the Enforcement Order stipulates the need for: (i) credit/debit/pre-paid card usage details; (ii) traffic card usage details; and (iii) video information collected through video data-processing equipment under Article 2, Item 7 of the Personal Information Protection Act” (Kim, n.d.).

The use of information on individuals for infectious disease control and privacy issues in Korea is characterized by (1) a wide range of information used in connection with the resident registration number, which is assigned to all citizens; and (2) a high ratio of cashless payments.

In Korea, according to the Resident Registration Act, which was enacted in 1962, a resident registration number (Hitachi, 2015) is assigned at the time of declaration of birth. A 13-digit number comprising the 6-digit date of birth, gender assignment number, the 4-digit area number, 1-digit birth declaration order, and a verification number, remains unchanged for life in principle. It is also compulsory for Korean citizens to obtain resident registration cards at the age of 17 years. The registration number is used for administrative work and is treated as a personal identifier in the private sector. Its use is currently limited to the scope stipulated by the Personal Information Protection Law, revised in August 2014, and includes credit card and cell phone numbers. Positive test results may also be cross-checked with the resident registration number.

In other countries with high ratios of cashless payments, information on individuals can be easily obtained by linking personal information to all types of cashless payment information. According to “the Cashless Vision” published by the Ministry of Economy, Trade and Industry in 2018, in a comparison of the ratio of cashless payments in countries world over, South Korea topped the list at 89.1% (Nomura Research Institute, 2018). However, in a report by the Nomura Research Institute, the figure was 96.4%.¹²

While referring to the response to the disclosure of personal information in South Korea, it will be necessary for Japan to consider (1) the scope of active epidemiological investigations and the obligation to co-operate as stipulated by the Infectious Diseases Control Law; (2) the relationship with the numbering system; and (3) the legal procedures based on the Personal Information Protection Law, while considering the request for, and disclosure of, personal information. With regard to (1), as a question of the scope of active epidemiological surveys based on the Infectious Diseases Control Law, there is a question of whether the follow-up survey of cashless payment information conducted in South Korea may also be conducted in Japan. However, as pointed out in Itakura (2020), cashless payment service providers cannot be included in the “other related parties” section 13 of the active epidemiological survey

¹² Article 15, Paragraph 6 of the Infectious Diseases Control Law was revised, and paragraph 7 now reads thus: “Any person who has been questioned or requested to conduct a necessary investigation pursuant to the provisions of paragraph 1 or 2 (excluding specified patients, etc., prescribed in the following paragraph) shall endeavor to cooperate with the said questioning or necessary investigation.” However, as there is no change in the subject of questions and investigations pursuant to paragraph 1 or 2, the subject of questions and investigations pertaining to active epidemiological investigations under Article 15-1 of the Infectious Diseases Control Law remains unchanged in the revised Infectious Diseases Control Law.

specified in the Act. The statutory obligation to co-operate in active epidemiological surveys of specified patients, etc., under the revised Infectious Diseases Control Law will be discussed later.

With reference to (2), in accordance with Article 9 of the “Act on the Use of Numbers to Identify Specific Individuals in Administrative Procedures” (Act No 27, 2013), the “Personal Number (My Number)” may be used for incidents related to recommendations or measures for hospitalization, burden of expenses, or payment of medical treatment expenses under the Infectious Diseases Control Act, which are specified by the ordinance of the competent ministry. In such incidents, the “Personal number (My Number)” may be used. On the basis of the Basic Resident Registration Act (Act No 81, 1967), the resident registration code may also be used.

As for (3), if the Personal Information Protection Law is used as the basis, it is permissible to provide personal data to improve public health and co-operate with public institutions. This issue has been discussed in Volume 1 of this paper.

2. The Obligation to Co-Operate with Active Epidemiological Surveillance of Specified Patients, etc., Under the Revised Infectious Diseases Control Law and Restriction on the Right to Privacy

1) Amendment of the Act on Special Measures against Pandemic Influenza, Infectious Diseases Act, and Quarantine Act

The “Act for the Partial Revision of the Act on Special Measures against a New Type of Influenza, etc.” (Act No 5, 2021) was promulgated on February 3. At the same time, the “Act on Special Measures against a New Type of Influenza, etc.”¹³ the “Infectious Diseases Act (Act on the Prevention of Infectious Diseases and Medical Care for Patients with Infectious Diseases (Act No 114, 1998)),” and the “Quarantine Act (Act No 201, 1951)” were partially amended and came into effect on February 13, 2021. The main amendments to the Infectious Diseases Control and Quarantine Laws were as follows:

- (1) Any new coronavirus infections will be deemed “a New Influenza and as other infectious diseases.” Measures related to these infections may be taken.
- (2) Information co-ordination among the national and local governments (reporting outbreaks from cities and wards with public health centers to prefectural governors and notification of the results of active epidemiological investigations to relevant local governments have been made mandatory. The use of electro-magnetic methods has been stipulated).
- (3) There has been a change in the legal status of overnight and home treatment (infectious diseases such as the new strains of influenza means that newly established provisions for requesting co-operation in overnight and home treatment for new infectious diseases have been specified by the Minister of Health, Labour and Welfare. The Quarantine Law also stipulates requests for overnight and home treatment, and other forms of co-operation necessary to prevent infection).
- (4) Review of hospitalization recommendations and measures (the scope of hospitalization

¹³ The outline of the revised law on special measures against pandemic influenza is as follows: (1) “Priority measures to prevent the spread of influenza” will be established to prevent the spread of influenza in specific areas that may have a serious impact on people’s lives and the national economy. (2) “Temporary medical facilities” that may be established during the declaration of a state of emergency can be opened from the stage when the government task force is established; (3) A non-penal fine (up to 300,000 yen) may be imposed for violating an order or for non-compliance with an order requesting to restrict the use of a facility during the declaration of a state of emergency; and (4) support for businesses and local governments (national and local governments) may be provided. support for local governments (The national government and local governments shall take the necessary financial measures to support businesses, and support for medical institutions and medical personnel. The national government shall deploy the necessary financial measures to support local governments. (5) The government will establish regulations on the responsibilities of the national and local governments in relation to the prevention of discrimination, and (6) The Cabinet will establish a Council for the Promotion of Countermeasures against H1N1 Influenza.

recommendations and measures will be limited to infectious diseases such as new strains of influenza and any new infectious diseases that have been specified by the Minister of Health, Labour and Welfare) stipulates a fine (up to 500,000 Yen) for non-compliance with hospitalization measures without justifiable cause or for fleeing from the hospital.

(5) To ensure the effectiveness of active epidemiological investigations, if a patient with a new type of influenza or other infectious disease does not co-operate with an active epidemiological investigation without a valid reason, the government may order the patient to comply and stipulate a non-penal fine (not exceeding 300,000 Yen), if the person receiving the order does not answer questions without a valid reason or gives false answers, or refuses, interferes with, or avoids the investigation without a valid reason.

(6) In case of an emergency, medical personnel (including medical institutions) may be required to co-operate with the “inspection body,” and if they fail to comply without a justifiable reason, they may be able to make a recommendation for enforced co-operation and publicly name the individual/s concerned.

2) Procedures for Ensuring the Effectiveness of Active Epidemiological Surveillance as Specified by the Revised Infectious Diseases Control Law

Where there is no confirmation of infection while investigating any situation, trends, and causes of infectious disease outbreaks (Article 15 of the Infectious Diseases Control Law: Active Epidemiological Investigations), penalties will not be imposed even if the subject does not respond to questions and investigations, etc., because of the wide scope of the subject, and the subjects of the active epidemiological investigations are only obliged to make efforts to co-operate with any questions and investigations (Article 15, Paragraph 6 of the former Infectious Diseases Law). The revised Infectious Diseases Control Law stipulates the procedure for issuing an order in the event where a patient with an infectious disease such as a new strain of Influenza does not co-operate with the active epidemiological survey without justifiable reasons, in order to ensure the effectiveness of the active epidemiological survey (Article 15, Paragraph 4 and 8 to 11, and Article 81 of the Infectious Diseases Control Law). While limiting the order to the minimum necessary threshold, provisions for written notification (Article 8-2 of the Infectious Diseases Control Law Enforcement Regulations) have been established.

The law provides for a non-penal fine of up to 300,000 Yen in the event where a patient with a new type of Influenza or other infectious disease, who has been ordered to respond to a positive epidemiological survey,¹⁴ fails to answer a question without a valid reason or gives a false answer, or refuses, interferes with, or avoids taking the survey without a valid reason (Article 81 of the Infectious Diseases Law). The law stipulates that the Prefectural Governor, etc., shall make a request (an administrative inspection) pursuant to the provisions of Article 15, Paragraph 3 of the Infectious Diseases Control Law, upon the prompt detection of infection in a patient, while taking into consideration the nature of the infectious disease, the infection situation in the area, the facilities and operations where the infectious disease has occurred, and other circumstances (Article 15, Paragraph 4 of the Infectious Diseases Control Law).

¹⁴ The targets are (1) patients, pseudo-patients, and asymptomatic pathogen carriers of class 1 infectious diseases, (2) patients and pseudo-patients of class 2 infectious diseases specified by government ordinance, (3) patients of new influenza and other infectious diseases, pseudo-patients who have good reason to suspect that they are suffering from such infectious diseases, and asymptomatic pathogen carriers, and (4) persons with findings of new infectious diseases.

3. The Applicability of Personal Information related to the “Examination of Personal Information Requiring Consideration”

Among the personal information requiring special consideration as stipulated by the Personal Information Act, Article 2 of the Enforcement Order for the Act on the Protection of Personal Information, includes the following statement: “a medical examination or other examination for the prevention and early detection of illness conducted on the individual by a physician or other person engaged in duties related to medical care (referred to as a physician, etc.)” Page 14 of the General Rules Guideline also provides examples of tests that fall under the category of “results of tests.” In responding to a new coronavirus infection, the acquisition of the results of a Polymerase Chain Reaction (PCR) Test is considered the acquisition of personal information requiring consideration.

However, the current Enforcement Order of the Act on the Protection of Personal Information and the General Rules Guidelines do not clearly state whether (1) “medical examinations and scheduled medical examinations for tests, etc.,” (2) “presence or absence of tests, etc.,” and (3) “refusal to undergo tests, etc.”¹⁵ are included within the scope of the “test results” and fall under the acquisition of personal information requiring consideration. Further, (1) “medical and scheduled medical examinations,” (2) “whether or not medical examinations have been conducted,” and (3) “refusal to undergo medical examinations” do not fall under the category of personal information requiring consideration because the “medical and other examinations for the prevention and early detection of illness conducted on the individual by a physician or other person engaged in medical-related duties (referred to as “physician, etc.”; under Article 2(2), the Cabinet Order)” “have not been conducted.” In the case of “positive/negative” test results, personal information regarding the “negative” test subject does not fall under the category of “medical history” under Article 2, Paragraph 3 of the Personal Information Law and is thus not personal information requiring consideration. However, the results of medical examinations and other tests fall under the description “medical examinations, etc.,” specified by a Cabinet Order under Article 2, Paragraph 3 of the Act. Therefore, regardless of whether the results of the examination are positive or negative, if personal information regarding the subject of the “negative” examination is handled together with the results of the relevant examination, it may fall under the category of personal information requiring consideration.

4. Infectious Disease Tests that are not Included in the Tests to be Taken and the Invasion of Privacy

It is also important to consider the issue of using specimens used in tests for infectious diseases in tests that include the confirmation of other infectious diseases. While considering this issue, we must refer to a case¹⁶ in which it was held that conducting a blood sample test without explicitly indicating the included HIV antibody test (Mutoh, 2006; Hanta, 1136; Yanagisawa, 2020)¹⁷ was an invasion of privacy without recognizing the reasonable need for the test, conducted without the consent of the individual concerned.

Obtaining information via HIV antibody tests as results, even though these HIV antibody tests were

¹⁵ There is a case in which two Japanese nationals who returned from Wuhan, China, on the first chartered flight on January 29, 2020 in the early stages of the outbreak of COVID-19 refused to be tested for the virus (but agreed later).

¹⁶ While considering the problem of using saliva specimens from patients who wish to undergo PCR for tests that include confirmation of other infectious diseases, Takamori et al. (2005) found that a study of confirmatory tests using saliva instead of blood specimens for HIV antibody tests produced results as good as those obtained with serum.

¹⁷ Tokyo District Court, May 28, 2003.

not included in the blood tests, which were clearly indicated to the individual, and for which consent was obtained, is a violation of the obligation to obtain personal information as stipulated under Article 17 of the Personal Information Law, and may also constitute acquisition beyond the scope of consent for the acquisition of personal information requiring consideration as stipulated under Paragraph 2 of the same Article. As this case law mentions that the information is “used” as a basis for rejection, if the test results are to be used for such a purpose, the consent of the individual concerned is mandatory as the use exceeds the scope necessary to achieve the purpose of use according to Article 16 of the Personal Information Law.

5. The Need for Thorough Safety Management Measures for Information Management related to Infectious Disease Control

To ensure the accurate collection of information for the determination of effective countermeasures against infectious diseases, personal information (personal data) should be securely managed and the privacy of the subject should be protected. The occurrence of a breach of the obligation of and negligence in security management, leakage, loss, damage, etc. will result in an infringement of the rights and interests of individuals and their privacy, as well as an attritional effect on the provision of information. Further, it will be a dis-incentive for the reliable collection of information.

With the publication of data on the number, age, and gender of infected people in order to encourage behavioral change, many problems have emerged. For instance, local governments have mistakenly published personal information that can identify specific, positive people, their contacts, and other related parties. In May 2020 (Nikkei Cross Tech, 2021), Aichi Prefecture released 495 cases online, followed by Kobe City (which published one case online in September 2020), Yokohama City (76 cases sent in error in October 2020), Nagoya City (published 100 cases and contact information online in December 2020), Morioka City (published one case online); Fukuoka Prefecture (shared 9,700 cases on the cloud for third parties to view), Nara Prefecture (published one case online), and Saitama Prefecture (published 191 cases online). Fukuoka Prefecture shared the information of 9,700 people on the cloud so that a third party could view it. Nara Prefecture published the information of one person online and Saitama Prefecture published the information of 191 people online.

The Infectious Diseases Control Law includes a provision for the obligation of confidentiality for “secrets” learned in the course of duty (Article 73, the same law). However, there are no special provisions for safety management measures for “personal information” that is not considered “confidential.” Infectious disease-related information that falls under the category of personal information is subject to the Personal Information Law. However, there is also information that does not fall under the category of personal information (see “3 Applicability to Personal Information and Personal Information Requiring Consideration” in the previous section). It may be necessary to consider the appropriate management of personal information that is not included within the scope of confidentiality obligations under the Infectious Diseases Law. As many people have refused to provide information that is deemed a matter of personal privacy leading to the identification of the route of infection, the statutory obligation to co-operate in active epidemiological investigations has made it impossible to refuse co-operation on the grounds of the right to privacy. As long as there is uncertainty around whether the personal information provided will be managed securely and privacy will be protected, there will be cases of hesitation in providing information.

III The Use of Technology for Infection Control Purposes and Issues concerning Privacy

1. The Use of GPS Location Information

GPS location information is essential for (1) obtaining information on the movement history and routes of infected people (movement status confirmation); (2) proving that infected people have not moved (quarantine status confirmation); and (3) measuring trends in people going out (flow and stay) and aggregation density, to prevent the spread of infection and monitor the aforementioned people. In contrast, for exposure notification mechanisms such as contact confirmation applications, there are two different approaches: using short-range wireless communication (Bluetooth) without obtaining the location of the device, as is the case with COCOA in Japan, and using GPS location information, as is the case in China and Korea.

Location information may be provided by (1) mobile operators, etc. at the request of public institutions; (2) mobile operators, etc. at the request of the media or research institutions; (3) public institutions that receive and publish location information for the sake of preventing the spread of infectious diseases (public health); (4) media institutions for the purpose of reporting; and (5) research institutions for the purpose of academic research.

The provision on location information, etc. has been used in a manner that does not constitute the provision of personal and personal information, while giving due consideration to the privacy of individuals by presenting it as statistical information (Shishido, 2020).¹⁸ However, in the event of an outbreak of a Class 1 or other unknown infectious disease that may seriously affect the life and health of the public, it may be necessary to identify and confirm location information to contain the spread of the disease through early detection and isolation, close contact tracing, and investigation of the behavioral history of positive cases. Where location information is handled as “literal personal data,” it is necessary to clarify the procedures in advance, such as deciding the scope of permitted use. Although the Personal Information Law is considered to allow the use of location information in keeping with the exemption from the application of relevant provisions, etc., under particular laws and regulations it is necessary to consider location information large-scale personal data in emergency situations from the perspective of protecting individual privacy. It is essential to conduct privacy impact assessments and consider “privacy by design” (Menges et al., 2021; Muscato, YEAR).

2. Considerations Required to Resolve Concerns about the Introduction and Spread of Contact Confirmation Applications

With the spread of the pandemic, many countries have been considering the use of contact confirmation applications to prevent the spread of infection. These applications have been developed and implemented (Menges et al., 2021; Muscato, YEAR) as emergency measures. For the sake of countermeasures against the next infectious disease, which is undeniably coming in the future, we should continue to study the problems pertaining to the introduction and dissemination of contact confirmation applications, by drawing on lessons learned from the introduction and implementation of applications for the sake of countermeasures against COVID-19. Thus, this discussion has been divided into the following categories: (1) institutional issues; (2) social acceptability; (3) degree of compulsion to

¹⁸ Provides details on the use of GPS location data in the fight against COVID-19, and points out problems in the publication of the results of providing data to the government. In the past, information on mobile spatial statistics was subject to a high level of privacy protection measures based on NTT DOCOMO’s Guidelines for Mobile Spatial Statistics. NTT DOCOMO’s “Information on Mobile Spatial Statistics.”

use; and (4) means of promoting use.

1) Institutional Issues

It seems necessary to consider two aspects of the institutional challenges pertaining to contact confirmation applications: (i) measures to dispel the sense of caution in the management of information by the state; and (ii) the stable operation of the system for contact confirmation and notification. This issue was discussed in detail during the establishment of the Basic Resident Register Network and the My Number System. The new COVID-19 contact confirmation application, “COCOA,” has general trust problems within the government (Habuka, 2020). The Japanese version of the contact confirmation app is a “device-matching type” (Personal Data Protection Committee, 2020) that does not acquire location information. After stating that most of the information handled in COCOA does not fall under the ambit of “personal information,” the Personal Information Commission has indicated that if the business involved in the app handles personal information, it should pay attention to the items listed in Table 2 and make them public. The Personal Information Commission has indicated that it is desirable to make this policy public (Personal Data Protection Committee, 2020). Issues pertaining to COCOA and personal information protection, including the fact that the “processing number of a positive person” and “diagnosis key” obtained by the MHLW fall under the ambit of personal information, under the Act on the Protection of Personal Information of Administrative Organs, were discussed in the previous part of this paper (III Standards for the Collection and Publication of Infectious Diseases-Related Information 4. Novel Coronavirus Contact Confirmation Application COCOA).

As for institutional issues in relation to privacy protection, the “Privacy and Security Assessment and System Operation Considerations for ‘Contact Confirmation Application and Related System Specifications’” ((Expert Panel Meeting on Contact Confirmation Application, 2020) describes the application of the Personal Information Protection Act for Administrative Organs and the Personal Information Act. However, confirming the content and direction of the implementation of specific privacy impacts and security assessments is not possible. To guarantee the right to privacy, the My Number system introduced both a mechanism to prevent the centralized management of information by the state and procedures for privacy impact assessment (specific personal information protection assessment). As pandemic responses require urgent and immediate action, this centralized management of information by the national government is essential for effective infection control, and information management and sharing through HER-SYS, including privacy impact assessment and the use of personal information. There is a difference between the use of information for the “improvement of public health” and that for “public interest in combating infectious diseases.” The former is a risk-management approach to disease prevention, and the latter is a crisis management response to the emergence and spread of infectious diseases. The main idea here is that the implementation of a privacy impact assessment should be linked to a consideration of measures for dispelling the sense of caution around information management by the state, as indicated in (i) above. As for the implementation of the Privacy Impact Assessment, knowledge of the Specific Personal Information Protection Assessment based on the Number-Use Law (the umbrella name under which the My Number system operates) can be used, and the “Information Technology - Security Technology - Guidelines for Privacy Impact Assessment (JIS X 9251:2021 (ISO/IEC 29134:2017)),” established on January 20, 2021, can be relied on.

The use of information may be hindered if different procedures for handling information are legally

established in both the public and private sectors. Subsequently, the “Draft Law on the Development of Relevant Laws for the Formation of a Digital Society” was approved by the Cabinet on February 9, 2021. To implement any measures for the formation of a Digital Society in accordance with the Basic Act on the Formation of a Digital Society, this bill made necessary improvements to relevant laws such as the Act on the Protection of Personal Information and the Act on the Use of Numbers to Identify Specific Individuals in Administrative Procedures. The three laws, namely the Personal Information Protection Act, the Act on the Protection of Personal Information of Administrative Organs, and the Act on the Protection of Personal Information of Incorporated Administrative Agencies, etc., are integrated into one law, within the Act on the Protection of Personal Information.¹⁹ The common nationwide rules for personal information protection systems of local governments are clarified in this integrated law, and the overall jurisdiction is centralized in the PPC. This new law stipulates some common national rules for the personal information protection systems of local governments, and takes measures such as centralizing the overall jurisdiction in the PPC.

Table 2: The Personal Information Protection Committee’s approach to the use of contact tracing applications as a countermeasure against COVID-19)

1) Are the purposes of the use of personal information to be acquired specified as clearly as possible, and indicated clearly to the users in an easily understandable manner, and will the consent of the individual for the acquisition of personal information requiring consideration and the provision of personal data to third parties be obtained?
For example: Please note here that the position of the application in the overall system of infection control, the fact that personal data are obtained for the purpose of infection control, the purpose and method of use of each data item, the third party to whom the data are provided and the reasons for this, the purpose and method of use of the third party to whom the data are provided, etc.
2) Are we obtaining data that are not necessary for the purpose for which they are to be used, or providing them to third parties that are not required?
3) When it is no longer necessary to use the data acquired, are they to be deleted without delay?
For example: Is the period of storage of the concentrated contact-history data set at an appropriate length while taking into account any epidemiological considerations, and will there be an assurance that the data will be deleted after the relevant period?
4) Are there adequate data security measures and are employees and contractors appropriately supervised?
5) Is there a system in place to respond to user queries and complaints?

One of the reasons citizens are so hesitant to use the information systems introduced by the state is that they are wary of and resistant to information management by the government. This hesitation

¹⁹ (1) The Personal Information Protection Law, the Personal Information Protection Law for Administrative Organs, and the Personal Information Protection Law for Independent Administrative Agencies will be integrated into a single law, and the personal information protection systems of local governments will be unified under the jurisdiction of the Personal Information Protection Commission by establishing common rules nationwide in the integrated law. (2) To unify regulations in the medical and academic fields, national and public hospitals, universities, etc. will, in principle, be subject to the same rules as private hospitals, universities, etc. (3) To comply with the sufficiency assessment of the GDPR, including academic research, the exemption for academic research will be elaborated upon as an exception for each obligation, rather than a uniform one. (4) The definition of personal information should be unified among national, private, and local governments, and the rules on the handling of anonymized processed information by administrative bodies should be clarified.

stems from concerns about the so-called Big Brother phenomenon. However, the problem is not so much about Big Brother itself as it is about the lack of progress in creating properly accountable information management IT infrastructure within the government (see Section 2: Notifications and Measures under the Infectious Diseases Control Act of Japan in Part III: Standards for the Collection and Publication of Information related to Infectious Diseases, in the first part of this report, including the use of fax notification procedures.)

With regard to the defects related to COCOA's contact notification (see 1 Institutional Issues above), the problems within the development of the system right from application to implementation, and subsequent verification, have been pointed out already. It is necessary to investigate and verify the causes of the defects in the system concerned and the causes and factors that led to the failure of the system in recognizing these defects. It is essential to scrutinize the defects and their causes from technical and institutional perspectives, respectively, and identify ways to prevent their recurrence.

The problems with the institutional aspects of the COCOA failure must be examined closely as a means for realizing the effectiveness and sophistication of contact confirmation and tracing technology in future infectious disease control. It will be necessary to confirm whether the current system in Japan is capable of coping with and responding to such a situation when a new information system is established in an emergency. Government procurement procedures and budget execution methods should also be examined, as the fundamental issue underlying the problem is not just a matter of application development but also concerns the institutional challenges and weaknesses that Japan faces in dealing with emergencies, which are the real issues here. It may be ideal to achieve the construction of perfect information systems and the development of perfect applications. However, in reality, they will inevitably have bugs and defects. To prevent such problems from occurring, it will be necessary to verify the implementation of any system in advance, and to check the status of problems after implementation and make improvements by adopting the Plan, Do, Check, Act (PDCA) cycle. At the time of writing, COCOA's failures had only been reported in the press. The author is awaiting further verification and a rigorous review and assessment of whether the management system has been functioning properly, and a clarification on the underlying factors that will be important for the future use of effective contact verification and tracing technology in infection control.

2) Social Acceptance

What everyone in society generally considers necessary may not be socially acceptable. The threshold of social acceptability is even higher when new technologies are used. Social acceptability overlaps with institutional issues like the protection of personal data. However, this must be considered in relation to privacy protection awareness. Installing contact confirmation apps will enable one to check his/her contact status with others. It will be mandatory for active epidemiological investigations to provide necessary contact details to prevent the spread of infection. However, the susceptibility of many people implies that they may not wish to have their contact details checked in the first place. The legal interest to be protected here is the right to privacy. However, this should also be considered from the perspective of "personal autonomy," that is, the protection of rights and interests related to self-determination. The idea that intervention in the self-determination of an individual should be accepted because of the risk of contagion when there is a high possibility of the seriousness of a present infectious disease (Ohta, 2020) and that "if an individual takes the best choice for the realization of his self-interest

from his own point of view, there may be undesirable consequences for society (the so-called the Fallacy of Synthesis)” (Oya, 2015). The respect for the right to self-determination of individuals in the event of a pandemic equivalent to a Category One Infectious Disease must be examined separately to determine whether it is socially acceptable in such situations.

3) Degree of Compulsion to Use (Pandemic Control) Apps

To promote the use of apps, the degree of compulsory/obligatory use may be set in stages, such as comprehensive compulsory use, compulsory use in specific environments, and voluntary use. Apps may be used for transportation and as a benefit (a) for domestic use and (b) as a pre-requisite for entry into another country. The level of coercion in infectious disease control should be determined according to the type of infectious disease. Considering examples of these combinations for; (A), the requirement to install the apps as a condition for leaving the country under curfew; (1 (a)), the use of the apps as a condition for entry into the country to exempt the period of isolation after entry or to check movement status within the country; (1 (b)). (B) could be conditional on a period of actual use of the apps as a condition for payment of benefits (1 (a)), as a condition for use of certain facilities (1 (a)(b)), or as a request for introduction of the app to certain professions or industries to prevent cluster outbreaks (1 (a)).

4) Pre-Requisites for Promoting the Use of (Pandemic Control) Apps

The following conditions are necessary to facilitate the use of pandemic control apps: (i) the effectiveness of the apps’ operational functions; (ii) the effectiveness of the contact confirmation and notification functions; and (iii) the adequacy of information management. The absence of defects, the use of information within the scope specified in the policy, and appropriate management are considered pre-requisites. It is possible to consider (iv) a change in the way of thinking to promote usage. A points system may be effective in promoting use. Setting up a system, such as a “points system for co-operation in measures to prevent the spread of new COVID-19 infections,” could be beneficial, where points are accumulated by people who are judged to not have come in contact with other people, by using the contact confirmation application. Another benefit of such a points system, for example, is if Bluetooth is turned off. In this situation, the number of contacts will decrease, so it would be a positive step toward providing points and benefits according to the number of contacts avoided in a situation where Bluetooth is turned on. However, simply storing the smartphone in a bag that shields it from radio waves can reduce the number of contacts to zero, so it is not expected to be useful as a means of promoting usage.

A concrete example of the opposite line of thought is the use of surveillance cameras. Although everyone is aware that surveillance cameras are intended for surveillance purposes, automatic speed-enforcement devices that detect speeding vehicles not only provide the evidence necessary to arrest the drivers, but the presence of the cameras themselves also has a deterrent effect on speeding behavior. The initial purpose of this device was only to curb speeding. However, in Sweden, the government adopted a pragmatic “carrot and stick” solution. The Swedish Speed Camera Lotteries (The Medical Futurist, 2018) proposed to change this problem by filming these drivers and offered prizes to those who did not speed. It was ironic, because if there was no speeding at all, there would be no winners and the funds would be lost. Although everyone is aware of the effectiveness and need for contact confirmation applications, they are not actively used. Bearing this in mind, may we change the way we think and create a system that many people will want to use?

3. Biometric Identification and the Use of Biometrics

The use of biometric data in infectious disease control and in verifying the identity of a person in order to implement countermeasures against infectious diseases is challenging. We suggest that biometric data acquisition is also possible in infectious disease control: for example, by using “drones equipped with heat detection devices” (Dormehl, 2020). We will intentionally leave the discussion of this issue for another study.

IV Sewage Epidemiological Survey and Privacy

1) Expectations of the Sewage Epidemiological Survey

A sewage epidemiological survey is “a method of testing viral genes in sewage in a specific area or facility. Such a survey is considered to contribute toward the early detection of infectious disease epidemics in the target area or facility and to the understanding of the epidemic situation” (Torii et al., 2020). The usefulness of a sewage epidemiological survey was highlighted as early as in October 2007 by the Pharmaceutical Affairs and Food Sanitation Council. The survey concluded that proper treatment of sewage is one of the most effective means of preventing Norovirus Food Poisoning. Based on this, an additional survey was conducted by the “Research Committee on Virus Countermeasures in Sewerage Systems” in November 2008, to ascertain the actual behavior of the Norovirus in sewage treatment plants, evaluating the removal performance of current sewage treatment facilities, and studying Norovirus countermeasures in sewerage systems. The revised Infectious Diseases Control Law has added “new coronavirus infections” and “re-emerging Coronavirus infections” to the list of New Influenza and other infectious diseases. We must be prepared for their re-emergence. Thus, the effectiveness of the sewage epidemiological survey (Kitajima and Haramoto, 2020) is expected to be a method of being fully aware of any new epidemic situation.

The functions of sewerage systems in combating infectious diseases include (1) controlling the risk of infection and (2) potentially detecting the presence of viruses and bacteria (Kato, 2020). “The three main routes of transmission of infectious diseases are contact (oral), droplet and airborne. By discharging sewage, including excreta and domestic waste, into the sewerage system, modern cities have succeeded in reducing the chances of contact and droplet infections in particular.”²⁰ “However, it should also be pointed out that the concentration of sewage in drains and sewage pipes has led to the circulation of viruses and bacteria in the environment. Viruses in the sewage from homes and buildings may enter the sewerage system and may be re-introduced into humans from sewage treatment plants via rivers, oceans, and sometimes living organisms, causing contact (oral) infections.”²¹ The detection of new Coronaviruses in sewage is expected to help identify signs of the spread of infection. The COVID-19 Task Force of the Japan Society for Water Environment (Matsui, 2020) was established on May 5, 2020 to “collect and disseminate domestic and international information on the detection, elimination, and risk management of new Coronaviruses in sewage and the aquatic environment.” Since May 13, 2020, the Bureau of Sewerage of the Tokyo Metropolitan Government has been experimenting with the detection of Coronaviruses by collecting samples of sewage from sewage treatment plants.

²⁰ same as lvii

²¹ same as lvii

2) The Privacy of Identifiable “Biological Materials” to be Found in Water Drainage Systems

There is a US precedent²² that there is no reasonable expectation of privacy in investigating a quantity of waste-water that flows into a public sewer, the source of which cannot be ascertained. In Japan, the issue of waste-water flowing into the sewerage system and privacy has not been raised. Issues relating to this US precedent may be divided into “drainage/surface water,” “waste-water,” and “water distribution.” The object of consideration in the relationship between sewage epidemiological investigation and privacy in this paper is “waste-water.”²³ However, the “drainage/surface water” in which the virus is “detected”²⁴ as a result of the investigation can be considered “waste-water” as well. The above-mentioned US case law concluded that there is no place for privacy protection in terms of the interests of operators in monitoring effluents under the Fourth Amendment. There is also a view (Gable, 2020) that a different conclusion may be arrived at if the subject is an individual citizen.

With respect to water drainage and privacy, the following issues should be considered: (1) the limited scope of the survey and (2) the acquisition of “biological samples.” Thus, (1), a virus is detected in the drainage water of a house in a remote location, and (2) a “biological sample” is obtained for virus-testing and genetic analysis. If the “sequence of bases constituting Deoxyribonucleic Acid (DNA), collected from cells” (Article 1(1)(a) of the Enforcement Order for the Act on the Protection of Personal Information; Cabinet Order No 507 of 2003), which is one of the “personal identification codes” in Article 2(2)(i) of the Personal Information Act, is obtained, personal information may be obtained from drainage water.

The Cabinet Secretariat’s “Working Group on Prejudice, Discrimination and Privacy of the Subcommittee on Countermeasures to Combat Infectious Diseases of New Coronaviruses” (2020) is currently examining the issue of discrimination.²⁵ If the epidemiological survey data on drainage water obtained for public health purposes is used to identify and publicize areas where infection has spread, the issue of “discrimination” may arise, and if the survey targets are limited the issue of privacy may also arise.

V For an Adequate Response to Future Pandemics

This paper was written when an emergency was declared because of the surge in COVID-19 (Article 1-2-1 of the Supplementary Provisions of the Law). This declaration was issued and had not been lifted at the time of writing, in accordance with Article 32-1 of the Law concerning Special Measures against New Influenza, etc. Pandemics like COVID-19 may occur frequently in the future because of environmental destruction; it is still impossible to foresee the end of this infectious disease (WHO, 2020; Tabish, 2020; BBC 2021).

Even in the field of infectious disease control, various institutional, social, and technical challenges

²² *Riverdale Mills Corp. v. Pimpare*, 392F.3d55 (1st Cir. 2004), *United States v. Spain*, 515 F. Supp. 2d 860, 861 (N.D. Ill. 2007), *United States v. Hajduk*, 396 F. Supp. 2d 1216 (D. Colo. 2005).

²³ “Water drainage” refers to the removal of unwanted water. “Wastewater” refers to dirty water that has been used. For more information on the difference between waste water drainage and wastewater, please refer to the special feature in issue 18 of the journal “Water Culture,” titled “Is water drainage wastewater?” On the basis of the difference between water drainage and wastewater, the article includes discussions on the history of water drainage, its use, and the efficiency of irrigation drainage.

²⁴ If, while testing effluents for infectious disease control, a virus is “detected” and the effluent is considered “wastewater,” the “detection” (if it corresponds to the “detection” referred to in JISZ8462-1:2001 Detection capabilities of measurement methods – Part 1: Terminology and definitions) is also naturally considered wastewater.

²⁵ The revised Act on Special Measures against Pandemic Influenza and Other Related Matters establishes new provisions on responsibilities relating to anti-discrimination measures.

have been identified. There is no shortage of opinions pointing out the delays in acting on these issues, but at the time of writing, only a few studies (Evans and Clayton, 2020)²⁶ had analyzed the causes for these delays. The inadequacy of technical responses, such as the problems in obtaining and sharing information toward infection control and the failure of contact verification applications, has also been exposed, as described in this paper. However, failures are potential successes and may well provide valuable lessons in preparing for future pandemics.

While considering the measures and policies toward preventing the spread of infectious diseases, it is important to consider the risk of sub-clinical infections such as new coronavirus infections (i.e., infectious diseases in which symptomatic people are the main agents of transmission, but there is a risk of infection from asymptomatic carriers as well, including infected people in the incubation period before the onset of the disease; Ministry of Health, Labour and Welfare, 2021) and new infectious diseases that may seriously affect the lives and health of the public, such as Class 1 and similar infectious diseases. In the event of an outbreak of a new infectious disease, which is likely to have a serious impact on the lives and health of the population, the identification, monitoring, and tracing of symptomatic individuals alone may not be enough to monitor the prevalence and prevent the spread of the disease.

The amendment of the Infectious Diseases Act to provide for legal measures to ensure the effectiveness of active epidemiological investigations into the behavioral history of positive patients and the refusal to co-operate with requests and instructions has paved the way for future infectious disease control. However, even with the obligation to co-operate in active epidemiological investigations, it may not be possible to obtain sufficient information by merely interviewing the positive person or confirming the information provided by the infected person, and it may not be possible to confirm the necessary information. In such cases, it cannot be denied that the use of the personal data of any infected person may help enact the necessary measures to prevent the spread of infection. In the case of infectious diseases such as COVID-19, which may also be transmitted by sub-clinical patients, contact confirmation and tracing methods are effective in deterring the spread of infection. Therefore, in preparing to properly deal with cases of serious infectious diseases equivalent to a Class 1 Infection, which may be transmitted by sub-clinical infection, due consideration should be given to any case where it is unavoidable to restrict an individual's right to privacy in relation to the public interest of preventing the spread of infection, and the interest of protecting the privacy of the individual concerned. This is because such measures are likely to cause discrimination and prejudice, and may lead to serious problems directly related to both human rights and privacy violations.

To some extent, the issues surrounding the protection of personal data may be identified as issues to be considered within the scope of the personal data protection system. The issue of privacy protection is not only systemic but also requires a timely response to issues concerning the protection of the personal interests of individuals, remedies for violations of these interests, and other issues that cannot be dealt with through a quantitative and procedural perspective because the personal interests of individuals are qualitative and subjective. Acknowledging these difficulties, the author has used the ongoing problems surrounding COVID-19 as a guide to some of the issues related to the protection of personal information and privacy that must be considered in preparing for the successful management of any pandemics in the

²⁶ It notes that the severity of the pandemic is the result of delays in the FDA's response and in the implementation and deployment of testing.

future. We hope that the need for a shared awareness of the crisis and proactive preparation for the future that have been set out in this paper will not have to become a repeated process in the distant future.

References

- Corrigendum: COVID-19 Pandemic and Data Privacy: Can the EU and Japan Share App Data?
- Aizawa, Kiyoka, Nakajima, Toshinari, Yamano, Haruko, Nakanishi, Tadashi, Sugaya, Junichi, and Ogawa, Tokuo (2000). Can the ocular surface temperature be a core temperature indicator? *Journal of the Japanese Society for Physiological Anthropology* 5 (1).
- Allen, Anita L. (2020). What is Privacy? *GPSOLO* 37 (9): 11.
- BBC (2021). Stopping the Next One: What Could the Next Pandemic Be?" *BBC*. <https://www.bbc.com/future/article/20210111-what-could-the-next-pandemic-be>. (Accessed 27 September 2022).
- Brown, Elizabeth A (2020). A Healthy Mistrust: Curbing Biometric Data Misuse in The Workplace. *Stanford Technology and Law Review* 23: 253.
- Cohen, Julie E, Hartzog, Woodrow, and Moy, Laura. The Dangers of Tech-Driven Solutions to COVID-19. *Brookings*. <https://www.brookings.edu/techstream/the-dangers-of-tech-driven-solutions-to-covid-19/>. (Accessed 27 September 2022).
- Corona tracking by IT: South Korea discloses infected people's routes, *Mainichi Shimbun*, Tokyo Morning News, April 16, 2020.
- Dormehl, Luke (2020). Pandemic Drones that Can Detect Fevers and Coughing will Soon Take to the Sky. *Digital Trends*. <https://www.digitaltrends.com/cool-tech/draganfly-drones-detecting-covid-19/>. (Accessed 27 September 2022).
- European Data Protection Board (EDPB) (2020). Guidelines 04/2020 on the Use of Location Data and Contact-Tracing Tools in the Context of the COVID-19 Outbreak, Guidelines 04/2020. https://edpb.europa.eu/our-work-tools/our-documents/ohjeet/guidelines-042020-use-location-data-and-contact-tracing-tools_en. (Accessed 27 September 2022).
- Evans, Barbara J and Clayton, Ellen Wright (2020). Deadly Delay: The FDA's Role in America' Covid-Testing Debacle. *Yale Law Journal* 130: 78.
- Expert Panel Meeting on Contact Confirmation Application (2020). Privacy and Security Assessment and System Operational Considerations for Contact Confirmation Application and Related System Specifications. https://cio.go.jp/sites/default/files/uploads/documents/techteam_20200526_02.pdf. (Accessed 27 September 2022).
- Fujiwara, Natsuhito (2020). Amendment of the Law to Strengthen Countermeasures against New Coronavirus Infections in Korea. *Minor Special Feature: Countermeasures against New Coronavirus Infections* 10–11: 283.
- Gable, Lance (2020). Legal and Ethical Implications of Wastewater Monitoring of Sars-Cov-2 for Covid-19 Surveillance. *Journal of Law and Bioscience* 7 (1): 1–11.
- Habuka, Hiroki (2020). Architecture and Governance of the Japanese Version of the New Coronavirus Contact Confirmation Application. (1173): 16.
- Hartzog, Woodrow (2020). Coronavirus Tracing Apps are Coming. Here's How They Could Reshape Surveillance as We Know It. *LA Times*. <https://www.latimes.com/opinion/story/2020-05-12/coronavirus-tracing-app-apple-google>. (Accessed 27 September 2022).
- Helm, Anne Marie and Georgatos, Daniel (2014). Privacy and mHealth: How Mobile Health 'Apps' Fit into a Privacy Framework Not Limited to HIPAA. *Syracuse Law Review* 64: 131, 162.
- Hitachi Ltd. (2015). Research Report on Personal Status Registration Systems in Other Countries (Republic

- of Korea). Ministry of Justice: Research and Study on the Ideal System for Introducing the My Number System to Family Registration Affairs. *Ministry of Justice*. <http://www.moj.go.jp/content/001203264.pdf>. (Accessed 27 September 2022).
- Itakura, Yoichiro (2020). Cashless Payment and Personal Information Protection - A Study on the Relationship with Active Epidemiological Surveillance as a Countermeasure against COVID-19 (Novel Coronavirus Infection). *Law and Computers* 38: 57–66.
- Jao, Nicole (2020). Alipay developed China's national health code rating system. *Technode*. <https://technode.com/2020/02/17/alipay-developed-chinas-national-health-code-rating-system/>. (Accessed 27 September 2022).
- Jung, Kim Myung (2020). What Japan Can Learn from South Korea's Measures Against New Coronaviruses - (3) Information Disclosure. *NLI Research*. <https://www.nli-research.co.jp/report/detail/id=64275?site=nli>. (Accessed 27 September 2022).
- Kato, Saki. (2020). Infectious Diseases and Sewerage: Risks and Possibilities. *MRI*. <https://www.mri.co.jp/knowledge/column/20200623.html>. (Accessed 27 September 2022).
- Kim, Chang-Ho (n.d.) Legal Framework for Responding to Novel Coronaviruses in South Korea - Focusing on Behavioral Regulatory Measures. *Nichibenren*. https://www.nichibenren.or.jp/library/pdf/activity/international/library/study_covid_19/1_2_4.pdf. (Accessed 27 September 2022).
- Kitajima, Masaaki and Haramoto, Eiji (2020). Analysis of Novel Coronaviruses in Sewage Water. *Bunseki* 11: 411.
- Kodama, Haruo (2017). Ethical and Legal Responses to the Problem of Dual Use of Scientific Research. *Journal of Corporate Law* 6 (1): 18-37.
- Matsuda, K, Yoshitake, R, and Shimada, K (1985). A Racial Comparison of Physiological Responses During Work in High Temperature and High Humidity Environments. *The Annals of Physiological Anthropology* 4 (1): 71–73.
- Matsui, Yoshihiko (2020). Establishment of the COVID-19 Task Force of the Japan Society on Water Environment. *JSWE*. https://www.jswe.or.jp/pdf/COVID-19TF_JSWE.pdf. (Accessed 27 September 2022).
- Menges, Dominik, Aschmann, Helene, Moser, Andre, Althaus, Christian, Wyl, Viktor von. (2021). The role of the SwissCovid Digital Proximity Tracing App During the Pandemic Response: Results for the Canton of Zurich. *medRxiv* 21250972.
- Ministry of Economy, Trade and Industry (2018). Cashless Vision. *Ministry of Economy, Trade and Industry*. <https://www.meti.go.jp/press/2018/04/20180411001/20180411001-1.pdf>.pp10. (Accessed 27 September 2022).
- Ministry of Health, Labour and Welfare (n.d.) Guidelines for Pandemic Influenza and Other Influenza Preparedness in Businesses and Workplaces. *Ministry of Health, Labour and Welfare*. <https://www.mhlw.go.jp/bunya/kenkou/kekkaku-kansenshou04/pdf/09-11.pdf>. (Accessed 27 September 2022).
- Ministry of Health, Labour and Welfare. (2021). Guide to the Treatment of New Coronavirus Infections (COVID-19), Version 4.2. *Ministry of Health, Labour and Welfare*. <https://www.mhlw.go.jp/content/000742297.pdf>. (Accessed 27 September 2022).
- Mozur, Paul, Zhong, Raymond and Krolik, Aaron (2020). In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags. *The New York Times*. <https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html>. (Accessed 27 September 2022).
- Muscato, Lindsay. *Contact-tracking app prevents 600,000 infections in the UK - Oxford University*
- Mutoh, Hisashi (2006). Claim for Damages against the Metropolitan Police Department's Unauthorized HIV Antibody Test. *Horitsu Jihou* 78 (972): 82–83.

- Natta, Meredith, Chen, Paul, Herbek, Savannah, Jain, Rishabh, Kastelic, Nicole, Katz, Evan, Struble, Micalyn, Vanam, Vineel and Vattikonda, Niharika (2020). The Rise and Regulation of Thermal Facial Recognition Technology During the Covid-19 Pandemic. *Journal of Law and Bioscience* 7 (1): 1–17.
- Nikkei Cross Tech (2021). Personal Information of People Infected with Corona ‘Inadvertently Leaked’, A Factor in a Series of Leaks. https://www.nikkei.com/news/print-article/?R_FLG=0&bf=0&ng=DGXZQ OFK0139Z0R00C21A2000000. (Accessed 27 September 2022).
- Nomura Research Institute Ltd. (2018). Consulting Division, ICT & Media Industry Consulting Department, Financial Consulting Department FY2017 Industrial Economics Research Commissioned Project: Progress Report on Research and Study on Environmental Improvement for FinTech Diffusion in Japan: Recognition of the Current Situation in Japan and Abroad for Promoting Cashless Technology. Document 3.
- NTT Docomo (n.d.). Guidelines for Mobile Spatial Statistics. https://www.nttdocomo.co.jp/corporate/disclosure/mobile_spatial_statistics/guideline/index.html. (Accessed 27 September 2022).
- NTT Docomo (n.d.). Information on Mobile Spatial Statistics. https://www.nttdocomo.co.jp/corporate/disclosure/mobile_spatial_statistics/. (Accessed 27 September 2022).
- Ohta, Tadahiko (2020). Pandemic and Public Law Issues: The Distribution of Medical Care in Response to ‘Danger’: The Infectious Disease Law Tested by New Coronavirus Infections. *Jurist* (35): 40.
- Oya, Y (2015). Pandemics and Trust in Others. *Hōgaku Seminar* (723): 47.
- Personal Data Protection Committee (2020). The Personal Data Protection Committee's approach to the use of contact-tracing applications as a countermeasure against new coronavirus infections. *CIO*. https://cio.go.jp/sites/default/files/uploads/documents/techteam_20200509_07.pdf. (Accessed 27 September 2022).
- Press Release <https://mp.weixin.qq.com/s/amB7fBxLw8KSR9DcUsbTWg>.
- Quilty, Billy J, Clifford, Sam, Flasche, Stefan and Eggo, Rosalind M. (2020). Effectiveness of Airport Screening at Detecting Travellers Infected with Novel Coronavirus (2019-nCoV). *Eurosurveillance* 25 (5): 2000080.
- Richer, Jena M. (2020). Victims of Introspection: Insufficient Legal Protections for At-Risk Users of Automated Mental Health Apps. *Vermont Law Review* 44: 893.
- Sato, Mia (2021). Singapore's Contact-Tracking App Changes Course. It Can be Used in Criminal Investigations. *Technology Review*. https://www.technologyreview.jp/s/230403/singapore-police-now-have-access-to-contact-tracing-data/?fbclid=IwAR3oN9QGPN8_DcaXHgH72grpG-FJp2C19seEi0YL9ovywErS_CMf-ms48M. (Accessed 27 September 2022).
- Shishido, Jyoju. (2020). Pandemics and the Challenges of Public Law: The Legal Discipline of Information Flow under Pandemics. *Jurist* (35): 65–67.
- Suda, Yuko (2021). The International Politics of Data Privacy. *Keiso Shobo* 178.
- ‘Surveillance society’ revealed by corona countermeasures: Is it OK to expose personal information to this extent in South Korea? 26091, ‘I was in a love hotel’: Is South Korea giving out too much information on new virus patient? BBC (March 5, 2020) <https://www.bbc.com/japanese/features-and-analysis-51748587>.
- Tabish, Syed Amin (2020). COVID-19 Pandemic: Emerging Perspectives and Future Trends. *Journal of Public Health Research* 9 (1): 1786.
- Takamori, M, Komori, Y, Nakashima, N, and Chiba, H (2005). A Study on Non-Specific Reactions in HIV Antibody Tests Using Saliva. *Sundai Journal of the Japanese Society for Oral Science* 54 (2): 283–292.
- Terada, Mayu (2020). Utilization and Protection of Personal Information in the After-Corona Era. *Hōgaku Seminar* 82 (787).
- The Medical Futurist (2018). The Swedish Speed Camera Lottery and Healthy Living. *The Medical Futurist*.

<https://medicalfuturist.com/swedish-speed-camera-lottery-healthy-living/> (Accessed 27 September 2022).

Torii, Shotaro, Furume, Hiroaki, and Katayama, Hiroyuki (2020). A Step Forward Toward the Practical Application of Sewage Epidemiological Investigation of Novel Coronaviruses: Proposal of an Optimal Method for the Concentration and Detection of Novel Coronaviruses from Sewage. *U Tokyo*. https://www.t.uokyo.ac.jp/shared/press/data/setnws_202010231219143592261907_037085.pdf. (Accessed 27 September 2022).

U S Equal Opportunity Employment Commission (2020). Pandemic Preparedness in the Workplace and the Americans with Disabilities Act. *US Equal Opportunity Employment Commission*. <https://www.eeoc.gov/laws/guidance/pandemic-preparedness-workplace-and-americans-disabilities-act>. (Accessed 27 September 2022).

University of Yamanashi, National University Corporation, and Hokkaido University (2020). First Successful Detection of RNA of a New Coronavirus in Sewage Samples in Japan - Expectations for the Use of Sewage Epidemiological Surveys for Monitoring the COVID-19 Epidemic." *University of Yamanashi*. <https://www.yamanashi.ac.jp/wp-content/uploads/2020/06/20200626pr.pdf>. (Accessed 27 September 2022).

Working Group on Prejudice, Discrimination and Privacy, Sub-committee on Countermeasures to Combat Novel Coronavirus Infections, Summary of Discussions to Date by the Working Group on Prejudice, Discrimination and Privacy (November 2020).

World Health Organization (WHO) (2020). The Best Time to Prevent the Next Pandemic is Now: Countries Join Voices for Better Emergency Preparedness. *World Health Organization*. <https://www.who.int/news/item/01-10-2020-the-best-time-to-prevent-the-next-pandemic-is-now-countries-join-voices-for-better-emergency-preparedness>. (Accessed 27 September 2022).

Xu, April Xiaoyi (2020). But What If Big Brother's Surveillance Saves Lives? - Comparative Digital Privacy in the Time of Coronavirus. *Creighton Law Review* 54 (2020): 147, 148.

Yanagisawa, Takeshi (1989). Rescission of Job Offer on the Basis of HIV Infection and Invasion of Privacy: Sapporo District Court Decision, September 17, 1989 [Latest Court Case Study] Labor Law/ (Sapporo District Court Decision, September 17, 2019)". *Hōgaku Seminar* (783): 113.

Yokota, Akemi (2020). Pandemics and the Challenges of Public Law: Multistage Amendments to the German Infectious Disease Prevention Act and the Provision of Information to Citizens - Legal Responses to COVID-19 (Novel Coronavirus Infections). *Jurist* (35): 74.

Yuasa, Takemichi 2020. Personal Information Protection Challenged by Countermeasures against Infectious Diseases: Can 'Privacy and Public Can we design 'privacy by design'? *Diplomacy* 62: 50–55.

[This article was originally published in 'Journal of Law and Information System Vol.9, p.62-80 (2021) <https://doi.org/10.32235/alis.9.0_62>', and the above is the translated version.]

Acknowledgements:

[This work was supported by JST, Moonshot R&D Grant Number JPMJMS2011.]