Opinion on Statutory Regulations on the Use of Facial Recognition Systems by Public and Private Sector Organizations and Incorporated Administrative Agencies

September 16, 2021
Japan Federation of Bar Associations

I. Summary of the Opinion

1. The Government should exercise strict control as listed below over the use of facial recognition systems aimed at the general public, regardless of being used by public or private sector organizations or by incorporated administrative agencies, to ensure that their use of the systems will not violate the right to privacy and associated rights of citizens unjustifiably:
   (i) Prohibit, in principle, creating facial recognition databases and other data sources, and using the facial recognition system without the data subject's explicit consent.
   (ii) Set strict criteria for exceptional cases where public administrative agencies, private businesses, and incorporated administrative agencies may create facial recognition databases and other data sources, and use the facial recognition system.
   (iii) Provide effectual oversight by the Personal Information Protection Commission.
   (iv) Publicize basic information about facial recognition systems
   (v) Enact legislation embracing the protection of rights of data subjects who are likely to have been entered into the database by mistake
2. In circumstances other than the ones described above, that is, in terms of facial recognition systems to verify certain individuals, as well as the once-only cross-referencing comparing the facial entries in storage media with facial images of specific individuals who opt into the cross-referencing, i.e., facial images that will not be saved in the facial image datasets, the use of facial recognition technology—regardless of being used by public or private sector organizations or by incorporated administrative agencies—should be limited to cases where the following criteria are met to ensure that the right to privacy and associated rights of citizens will not be violated unjustifiably:
   (i) An explicit statute permitting the use is in place.
   (ii) The facial recognition system is not used for individuals who do not consent to the use.
   (iii) Individual consent is not mandatory and optional choices are available so that people will not be subjected to detriments even if they do not consent to the use.
   (iv) The organization with a facial recognition system installed notifies the Personal Information Protection Commission that the facial recognition system has been set in place and is in use.
3. At least, the following activities must be discontinued:

(i) Conducting police investigations using facial recognition technology even though there is no legislation that limits the scope of such investigations exclusively to investigation of serious organized crimes

(ii) Employing facial recognition technology at healthcare receptions where patients check-in using the Individual Number Card (with a photo).

(iii) Expanding the use of facial recognition data to a large extent by linking the Individual Number Card with the Health Insurance Card, etc., thereby further increasing the scope of facial recognition systems use.

In addition, collecting and cross-referencing facial recognition data in public administration even though verification by face photos is working, should not be permitted because there is no need to implement it.

II. Reasons for the Opinion

1. Operation of Facial Recognition Systems by Public Administrative Agencies, Private Sector Organizations and Others[2] and its Expansion

Use of facial recognition systems in Japan started when they were installed and operated at Kansai Airport and Narita Airport customs to prevent hooligans (those who cause trouble when watching football matches) from entering the country when the FIFA World Cup was co-hosted by Japan and Korea in 2002.

Since then, facial recognition systems have been used also by private sector organizations, such as theme parks, offering a service for their annual pass holders to register their facial recognition data in a "facial recognition database for annual pass holders" in advance so that they will be instantly matched by AI just by turning their face to the camera at the entrance and allowed literal "entry on sight." Other examples of such use include systems to match the data of concert ticket purchasers transmitted by them and stored in a facial recognition database with the face of those who attend the concert venue at the entrance to allow them entry to prevent such tickets from being resold at a higher price, or systems at bookstores and other stores to cross-reference the database of shoplifters with the face of the customers who visit the store in order to prevent shoplifting. Such uses of facial recognition systems are increasing.

The smartphone "iPhoneX" launched in 2017 introduced an identity verification system by facial recognition, and its verification accuracy was said to be 1000 times higher than verification by fingerprint. The accuracy is increasing year by year, but verification errors have not been reduced to zero. The improvement in accuracy will lead to accurate monitoring, which increases the

[2] "Others" is included to reflect the categorization under the personal information protection legislation of (i) private business operators, (ii) public administrative agencies, and (iii) incorporated administrative agencies. Incorporated administrative agencies also need to be subjected to regulations similarly to public administrative agencies.

seriousness of privacy violations in cases of misuse, while increasing the risks in case of a verification error due to the confidence in its accuracy.

Meanwhile, in the public sector, the issuance of individual number cards ("My Number" cards) started in 2016, in which facial image data capable of generating facial recognition data are stored on the IC chip[3], and such cards are issued by local governments only after it is verified that the facial image data of the applicant are sufficiently accurate to enable facial recognition.

Moreover, in association with the integration of individual number cards and health insurance cards that has been test operated since March this year and is to be put into full-scale operation as from October this year, the Ministry of Health, Labour and Welfare (MHLW) states that they will expand the use of card readers with a facial recognition function at medical institutions at the full expense of the government.[4] It is planned that a patient will place his or her individual number card on a card reader at the reception desk of the medical institution and a facial recognition system will check if the face of the patient captured by the camera built in the card reader matches the facial recognition data generated from the facial image data on the IC chip of the card. Furthermore, in respect of such use of the individual number card as a health insurance card, the government suggests abolishing paper insurance cards, stating that "we will aim at moving to a system operated with individual number cards only without the issuance of insurance cards in the future" (MHLW: "Proposed Arrangement for Operation, etc., of the Online Qualification Verification System (Overview) (June 2019 Edition)").

In December 2020, a schedule was indicated for the integration of the driver's license with the individual number card as of the end of FY2024. As a side note, as from 2007, an IC chip has been mounted on a driver's license, which stores the data of the facial image displayed on the surface of the card.

The individual number card system was supposed to be a system that would contribute to convenience of the general public, on the precondition that acquisition of the card would be voluntary, so that the lives of those who do not seek such convenience would not be hindered. But its integration with the health insurance card and the driver's license may practically force people to acquire an individual number card because their lives would be hindered without the card. Thus, with the rising convenience through the expanded use of individual number cards, the risk is high that submission by citizens of their facial recognition data to public administrative agencies will be de facto obligatory.

[3] https://www.soumu.go.jp/kojinbango_card/03.html

[4] It is stated in the "Q&A on the 'Implementation Guidelines for the Subsidy for the Development of Medical Care Provision Equipment'" by the Division for Health Care and Long-term Care Integration, Health Insurance Bureau, Ministry of Health, Labour and Welfare (July 3, 2020) that "if a card reader with the facial recognition function is not introduced, none of the expenses, including the expense for upgrading the online qualification verification system, etc., will be covered by the subsidy," indicating that strong guidance by policy measures is being made.

As described, social reality that is contrary to our proposals in the 2012 Opinion (Opinion Concerning the Legal Restrictions on Security Cameras) and the 2016 Opinion (Opinion Concerning the Legal Restrictions on Facial Recognition Systems) is expanding, under which the use of facial recognition data and facial recognition systems is expanding both in public and private sectors.

Such expansion of the use of facial recognition systems and changes in the environment accompanying the expansion are not taking place only in Japan, and there are examples such as in China that facial recognition systems are widely used by the state to monitor citizens.[5] Even in Japan there are concerns about such abuses, especially in light of a lack of appropriate regulations that impose restrictions on public administrative agencies.

Facial recognition systems do offer certain convenience and utility, but on the other hand, they will bring harmful effects on the rights to privacy and other civil liberties if they are used in an inappropriate manner.

2. Regulations on Facial Recognition Systems in Other Countries

(1) EU

Article 9, Paragraph 1 of the GDPR (General Data Protection Regulation) put into effect as of May 2018 stipulates prohibition of collection of biometric data, typically including facial recognition data, in principle, and exceptions provided for under Paragraphs 2 and 3 of the same Article are limited to cases where it is necessary to protect the vital interests of the person, or where it is provided for under the EU law or the domestic law of the member state and

[5] In an NHK news program dated February 26, 2018, an overview of security cameras and facial recognition technology in China was introduced as follows:
“In China, over 170 million security cameras are installed. Individuals are identified by facial recognition systems, and for example, if one crosses at a crosswalk ignoring a red light, he/she will be fined about 400 yen.

According to the explanation by a person in charge at a facial recognition system development company, 3,000 wanted persons have been arrested using financial recognition systems. At ATMs in China, cash can be withdrawn using facial recognition systems without a card or PIN input. They also keep an eye on excessive use of toilet paper at public restrooms. A person who is considered to be a dissident was identified by a camera in a subway in Beijing and arrested. A Chinese writer who is deemed a dissident says that they were constantly monitored.”

In facial recognition systems, data are processed at a high speed by AI. The computer network built around the security cameras using AI installed and operated by China is called “SkyNet” (the name is said to come from the Chinese saying, “heaven’s net has large meshes, but nothing escapes”) and is said to be capable of matching 3 billion faces per second.

There is also criticism that they are used to monitor the minority Uyghurs in the Xinjiang Uyghur Autonomous Region.

In 2019, in Hong Kong, demonstrators protesting an extradition bill took countermeasures to cover their faces with a mask to circumvent monitoring by the authorities using facial recognition systems. In October of the same year, the Hong Kong government enacted and enforced a mask ban ordinance to ban demonstrators from wearing a face mask or covering without taking legislative procedures by invoking the Emergency Regulations Ordinance for the first time in about 50 years. Wearing a mask, etc., to cover the face to avoid personal identification was prohibited and became punishable by imprisonment for a period of no more than one year, etc.

necessary for reasons of substantial public interests, and so on. Even in cases where data are collected and used by a private business operator, collection is not allowed without legislation by the parliament.

Further, the guidelines ("Guidelines on processing of personal data through video devices" of 2019) of the European Data Protection Board (EDPB), which is an advisory committee of the EU, also stipulates that access management using facial recognition systems at checkpoints of airports and buildings is allowed only with explicit prior consent of the users, and alternative means without using facial recognition systems must be provided for those who do not give consent. Moreover, it is also stipulated that the manager of security cameras must comply with a request from an individual who is a data subject to disclose video footage in principle.

Further, the Guidelines on Facial Recognition published in January 2021 not by the EU but by the Council of Europe stipulates that private companies may not use facial recognition technology at shopping malls, etc., for the purpose of marketing or crime prevention.

In 2013, it was revealed by Mr. Edward Snowden, a former staff member of the NSA (U.S. National Security Agency), that information on the behavior of people on the internet all around the world had been provided by digital platformers that are in a position to acquire the same to intelligence agencies thorough lawful procedures. In the light of this, the EU moved to strengthen regulations for privacy protection.[6]

In relation to the referendum on the United Kingdom's exit from the EU in June 2016 and the US presidential election in November of the same year that Cambridge Analytica, an election consulting company, was used by the winning side on each of those occasions, a question was posed that the elections may have been influenced by analyzing the personalities of individuals based on such information on the internet and guiding them to information supporting certain ideas.[7]

(2) United States

Unlike the EU that has put great importance on privacy protection, the United States has considered the free flow of personal information among private businesses per se as a freedom

[6] On October 6, 2015, the European Court of Justice invalidated the Safe Harbor Agreement, under which mutual transfer of personal data between the EU and the United States had been allowed on the premise of an equal level of personal information protection between them based on the EU Data Protection Directive 95. The EU considered it problematic that the system allowed the government including the intelligence agency easy access to digital platformers (easiness of government access), and the GDPR which was put into force in May 2018 was established to prevent the EU from being affected by such situation for privacy protection. Then, the Privacy Shield Decision provided to replace the Safety Harbor Agreement was also invalidated by the European Court of Justice on July 16, 2020. The EU has been consistently calling on the United States and other countries for a level of privacy protection equivalent to that provided by the GDPR.

[7] For more details on micro-targeting which altered the voting behaviors of people by meticulously providing them with advertisements that are most effective to their personalities captured on SNS, see "AI vs. Democracy: Depth of Increasingly Sophisticated Manipulation of Public Opinions" (NHK Publishing).

of expression and its position as a key component of the Constitution has been highly regarded. The digital platformers referred to as GAFAM have been accumulating and commercially utilizing personal information, embodying such an idea.

However, since the Cambridge Analytica case brought to light that the free flow of personal information rather threatens to distort the formation of sovereigns' decision-making and infringe on the freedom of expression, a shift in values is said to be taking place in the United States towards the necessity for restrictions on the flow of information (American way of "freedom of expression") based on the rights of privacy.[8] Today, the digital platformers are expressing their intention one after another to change their policies to restrict the use of facial recognition systems and protect privacy.[9]

The California Consumer Privacy Act which came into effect in January 2020 stipulates that business operators must disclose the purpose for which they use the personal information they collect and use as well as the scope of such use, and must suspend the sale of and delete such information if requested ex post.

Further, in San Francisco and other places, the use of facial recognition technologies by the police and other municipal organs is prohibited.

And the states of Texas, Illinois and Washington have legislated to restrict services using facial recognition systems. For instance, the Biometric Information Privacy Act of Illinois prohibits private companies and private entities from acquiring biometric information including facial recognition data without prior consent of the data subject, etc.

3. Necessity of Legal Regulations on Facial Recognition Systems in Japan

As we discussed in the 2016 Opinion, under the current facial recognition systems, if a facial recognition database of specific surveillance targets is created in advance, it is possible to generate facial recognition data from the facial image data collected and automatically conduct searches and match them with the database using AI. If facial recognition data are subjected to searches and matches, individuals will be comprehensively targeted for surveillance from the past into the future and it will be possible to identify their action histories in detail.

Thus, facial image data and facial recognition data that are biometric information which enables personal identification in a far more accurate manner than fingerprints are highly sensitive information equivalent to DNA information.

Furthermore, since it is difficult to acquire fingerprints or DNA information without an action such as fingerprinting or submitting DNA materials, etc., consent to such action is likely to be

[8] Based on the content of a lecture given by Professor Tatsuhiko Yamamoto (Keio University) held on July 20, 2020, organized by the JFBA's Human Rights Protection Committee.

[9] For example, Microsoft Corporation recommended on December 6, 2018 that the government needs to promptly impose legal regulations on the use of facial recognition systems by private business operators.
https://news.microsoft.com/ja-jp/2018/12/13/blog-facial-recognition-its-time-for-action/

ensured. However, facial recognition data can be generated without being noticed by the data subject just by passing in front of a security camera that records at a certain degree of accuracy or higher, and facial image data have been collected for the purpose of visual confirmation of identity (typically, when acquiring/renewing a driver's license) since before facial recognition systems were put into practice, but such thoughtless handling of data has continued irresponsibly even after the high sensitivity of facial image data and facial recognition data became a problem.

In other words, collection of facial image data, which was not a problem before the practical application of facial recognition systems, must be regulated by strict criteria as pointed out in the 2016 Opinion now that facial recognition systems have been put into practice and the police actually utilize this data for investigations, and it is the standard way of thinking in democratic countries represented by the EU member states that such data must not be used freely by public authority without such laws.

The JFBA has been calling for legal discipline over fingerprints, DNA databases, security cameras, facial recognition databases, etc., and facial recognition systems, which are nothing but minimum requirements that must be cleared automatically by any democratic country as a "law-governed state." But no such legal discipline has yet been established to date and the authority of the police and other public administrative agencies have a free hand to use such sensitive information. Such situations must be rectified immediately.

It is absolutely necessary to enact a law and restrict the use of facial recognition systems.[10]

4. Criteria for Legally Permitted Use

Strict criteria must be applied for collection, use and storage of facial recognition data and facial image data accurate enough to generate the same, treating them as highly sensitive information.

Restrictions on their use must be based on the strictest judicial review standard[11] provided as

[10] There is some misunderstanding that collection and use, etc., of personal information are lawful if the Act on the Protection of Personal Information or the Act on the Protection of Personal Information Held by Administrative Organs, etc., are complied with. However, as discussed in the "Opinion on Internet Map Retrieval Systems Containing Numerous Images of People and Residences" released by the JFBA on January 22, 2010, it is established as a legal precedent that violation of privacy will constitute a tort and this has not been particularly relaxed even after the enforcement of the Act on the Protection of Personal Information, etc. (see Supreme Court judgment of November 11, 2005). Figure 2 on Page 4 of the "Guidelines on the Use of Camera Images" (version 2.0) stipulated by the Ministry of Internal Affairs and Communications in March 2018 also shows the "scope to be considered from the perspective of privacy protection" by business operators as a scope larger than the "scope to be protected by the Act on the Protection of Personal Information," i.e., the government also admits that the scope of required privacy considerations is larger to avoid a tort. The GDPR provides for the prohibition in principle of collection of biometric information, etc., under Article 9, separately from the General Provisions, and requires special legislation to the same effect that additional regulations are necessary for privacy protection considering the sensitivity of the information.

[11] Refers to the standard that requires that the purpose shall be essential and compelling interests and the means shall be limited to the minimum necessary to achieve such purpose. ("Constitution 5th Edition" by Nobuyoshi Ashibe /Supplemented and modified by Kazuyuki Takahashi; Iwanami Shoten, P.124).

a standard of constitutionality review for sensitive information.

Since the current facial recognition systems are categorized into several types including, for example, the following, regardless of whether they are used in the public sector or by private organizations, the criteria for use should be discussed separately for the respective types.

(i) Cases where a facial recognition system is used aiming at a large number of unspecified persons: a typical example is a system to cross-reference a facial recognition database (so-called "black list") with a large number of unspecified persons.

(ii) Cases other than (i), in other words, facial recognition data are used for certain individuals: a typical example is a system to cross-reference a facial recognition database of qualified persons who gave prior consent with specific persons who opt into such cross-referencing.

(iii) Systems for once-only cross-referencing without creating a facial recognition database that compare facial recognition data in storage media with specific individuals who opt into such cross-referencing.

We make a type-by-type discussion as follows:

(1) Cases where a facial recognition system is used aiming at a large number of unspecified persons

[A] Restrictions on the creation of facial recognition databases, etc., and the use of facial recognition systems

A typical example of such systems falling under (1) is a facial recognition system utilized for investigation of organized crime by the police that we discussed in the 2016 Opinion. The abovementioned strictest judicial review standard should be applied to such use by the police, and current Opinion does not intend to modify the 2016 Opinion. However, since a standard equivalent to such standard must be provided by law also for uses by public administrative agencies other than the police, we make a recommendation in the current Opinion.

As we discussed in the 2016 Opinion that the creation of facial recognition databases and the use of facial recognition systems should be limited to investigation of "serious organized crime," it must be strictly interpreted whether the interests concerned are essential and compelling enough to justify the creation of facial recognition databases, etc., and the use of a facial recognition system.

In particular, it should not happen that people are treated as criminal suspects or illegal immigrants at all times because it would not only infringe on their privacy but constitute a violation of their right of honor.[12]

[12] According to the "Camera/Facial Recognition Services and Trends of Regulations in Western Countries" by Yusuke Koizumi, the FBI performs cross-referencing with passport application photos, photos of visa applicants, photos on

(a) Public Administrative Agencies

Creation of facial recognition databases and other data sources and use of facial recognition systems by public administrative agencies shall be allowed only when an explicit consent of the data subject has been obtained in principle.

Further, exceptions to such principle where the data subject's consent is not required shall be limited to cases where an extremely important administrative purpose equivalent to investigation of a serious organized crime exists, such as preventing entry of a terrorist into Japan, and the use of a facial recognition system is absolutely necessary as a means to achieve such purpose. Spatial limitations shall be applied also to facial image data based on which facial recognition data for cross-referencing are generated, such as that for airports where such data are absolutely necessary in achieving administrative purposes, and facial image data collected elsewhere should not be used.

Furthermore, to prevent an unreasonable expansion of the creation of facial recognition databases and the installation and use of facial recognition systems based on own judgments of public administrative agencies as to whether the abovementioned criteria are met or not, administration by law must be ensured to make sure that public administrative agencies may create facial recognition databases and install and use facial recognition systems only in cases where the same are specifically and expressly permitted by law. In other words, once a law is established to regulate the use of facial recognition systems by public and private sector organizations, it will be possible to supervise private business operators and others through permissions of the Personal Information Protection Commission as discussed later. However, for public administrative agencies, a separate enabling legislation will be necessary according to the principles of a law-governed state and rule of law. Without such legislation, it is unlikely to be avoided that facial recognition systems will be operated for administrative purposes that are deemed necessary based on the public administrative agencies' own judgments. It is absolutely necessary to enact a separate enabling act stipulating strict exceptions similarly to the law to regulate the use of facial recognition systems for police investigation suggested in the 2016 Opinion.

(b) Private Business Operators and Others

Criteria equivalent to those described in (a) above should be applied to private business operators and other organizations other than public administrative agencies.

In Japan, systems actually used in this manner include systems at bookstores to cross-

driver's licenses, etc., and the New York City Police performs cross-referencing with information posted on SNS such as Facebook and Instagram. Such practice is problematic because it is equivalent to subjecting innocent good citizens to investigation at all times as potential criminals. The 2016 Opinion calls for requirements of temporal and spatial proximity to the crime scene and collection of data by warrant.
https://www.i-ise.com/jp/information/report/2019/20191029_facial_recognition.pdf

reference a facial recognition database of shoplifters, etc., with visitors. In light of significant violations of privacy and the right of honor of individuals incurred once they are listed on such a blacklist, if we were to set criteria for those who may be registered on a facial recognition database, they should be limited to such individuals who have committed a crime against the user of the relevant facial recognition database and an explicit consent of the intended registrants should be obtained.

Further, since the use of such facial recognition system subjects many innocent visitors to cross-referencing with the database of shoplifters at all times, certain restrictions must be applied. Thus, various criteria must be fulfilled to ensure that visitors who do not want to be cross-referenced are made aware of its existence and able to avoid it and to reduce violation of privacy of other visitors. Such various criteria include the following: the probability is considerably high that crimes will be committed at the place of such installation; there are no alternative means that are less detrimental to rights to privacy, etc.; the facial image data based on which facial recognition data for cross-referencing are generated shall be limited to those collected at the place of installation; the installer has the administrative authority over the place where searches and matches by a facial recognition system are conducted at all times; and permission of the Personal Information Protection Commission shall be obtained for the creation of a facial recognition database, etc., and the installation and management of a facial recognition system.

(c) Matters That Should Be Provided for by Law

Based on the discussion above, it is necessary to establish a law containing the following provisions for the restrictions on the creation of facial recognition databases, etc., and the use of facial recognition systems:

(i) Creation of a facial recognition database, etc., and use of a facial recognition system without an explicit consent should be prohibited in principle.

(ii) Public administrative agencies should be permitted to create a facial recognition database, etc., and use a facial recognition system without obtaining consent of the data subjects only when the following criteria are fulfilled:

a. Only a very limited category of individuals, such as terrorists, may be registered in a facial recognition database.

b. The targeted administrative purpose shall be an extremely important one, such as checking for terrorists, etc., at the immigration counter.

c. The use of a facial recognition system is absolutely necessary to verify personal identity.

d. The facial image data based on which facial recognition data for cross-referencing are generated shall be limited to those collected at a place where such data are absolutely necessary to achieve the administrative purpose, and no facial image data collected elsewhere shall be used.

e. The creation of a facial recognition database and the installation and use of a facial recognition system are specifically and expressly permitted by law.

(iii) When a private business operator or an organization other than public administrative agencies creates a facial recognition database, etc., and uses a facial recognition system, the following criteria must be fulfilled:

a. Registrants in a facial recognition database shall be limited to those who have committed a crime against the user of such facial recognition database and an explicit consent shall have been obtained from such registrants.

b. The probability is considerably high that crimes will be committed at the place where a facial recognition system is installed.

c. There are no alternative means that are less detrimental to rights to privacy, etc., than the use of a facial recognition system.

d. The facial image data based on which facial recognition data for cross-referencing are generated are limited to those collected at the place of installation.

e. The installer has the administrative authority over the place where searches and matches by a facial recognition system are conducted at all times.

f. Permission of the Personal Information Protection Commission shall be obtained for the creation of a facial recognition database and the installation and use of a facial recognition system.

[B] Conditions for the Operation of Facial Recognition Systems

After limiting the creation of facial recognition databases, etc., and the use of facial recognition systems to such cases where the criteria stipulated in [A] above are fulfilled, the following conditions similar to those proposed in our 2012 and 2016 Opinions must be fulfilled in their operation not limited to the direct use of facial recognition systems, in order to protect privacy rights of those subjected to cross-referencing:

(i) Facial recognition data to be cross-referenced against a facial recognition database shall be generated only at the time of such cross-referencing and shall not be stored after the cross-referencing is over, and the facial image data acquired at the place of installation of a facial recognition system shall be immediately discarded when such data are no longer necessary for the administrative purpose or the purpose of such installation by the private business operator, etc.

(ii) A registration period shall be set for the facial recognition data registered in a facial recognition database, and the data shall be immediately deleted upon expiration of such period.

(iii) A facial recognition system shall not be used for any other purposes.

(iv) The organizations using a facial recognition system shall be made public. Further, if a facial recognition system is operated using security cameras currently in place, it must be explicitly indicated at their locations that the facial recognition system is in operation, as well as its purpose, the responsible person, and his/her contact information.

[C] Other

The following must be also complied with in order to prevent unjust violation of privacy such as by erroneous listing in a facial recognition database:

(i) Supervision by the Personal Information Protection Commission

It shall be ensured that the Personal Information Protection Commission can check regularly and effectively whether the collection of facial image data, the generation, acquisition, use and disposal of facial recognition data, the creation of, registration at and deletion from the facial recognition database, and the use of a facial recognition system, etc., are appropriately conducted by the public administrative agencies, private business operators and others.

(ii) Disclosure of Basic Information

The installer shall disclose the mechanism of a facial recognition system and the accuracy of its searches and matches on a regular basis.

(iii) Rights of the Data Subjects

Individuals who might be erroneously registered in a facial recognition database shall be granted the right to request disclosure and the right to request deletion.[13] [14] If it is difficult to directly guarantee such rights, it shall be ensured that they can request the Personal Information Protection Commission to verify the legality on their behalf.

As for the latter half of the preceding paragraph, even in cases where it is difficult for the installer to communicate directly with the disclosure requester, it shall be ensured that, upon receipt of such request, the Personal Information Protection Commission can check on behalf of the requester whether he/she is registered and the grounds, etc., for the

[13] The Tokyo High Court judgment of March 24, 1988 also recognized the right to request deletion, stating that "if personal information held by another person is untrue and unauthorized to the extent it exceeds the socially tolerable limit, and the individual suffers damage exceeding the socially tolerable limit due to the same, there must be cases where such individual may request such other person to correct or delete such untrue or unauthorized information based on his/her right of honor or personal rights."

[14] The JFBA has been pointing to the importance of the right to request disclosure and the right to request deletion: for instance, on March 9, 2016, we requested the Director of the National Police Agency to reply to an inquiry of a petitioner as to whether he was registered in the "Organized Crime Group Information Database" and delete the data if it was found to be registered erroneously, as it was likely that he was erroneously registered as a former member of an organized crime group although he had never been a member and was suffering detrimentally such as being treated as such in a prison for inmates with advanced criminal tendencies based on the information.

registration if registered, and request for verification of its legality.[15]

(2) Cases other than (1), i.e., where a facial recognition system is used for certain individuals

A typical example is a system to cross-reference a facial recognition database of qualified persons who gave prior consent with specific persons who opt-into such cross-referencing.

There are no particular problems with the use of facial recognition systems on smartphones and the use of facial recognition systems at theme parks or concert venues for the convenience of those qualified to enter such places with their voluntary consent. However, if the system is used in a manner that those who do not give consent cannot receive services, they will be de facto forced to submit information that enables verification of their identity with an accuracy that is 1000 times higher than that with fingerprints. Thus, there is an issue of whether one can claim that the conditions of necessity and appropriateness are met to prevent a tort under Article 709 of the Civil Code from arising, as in the case of requesting compulsory submission of fingerprints.

In the first place, once a facial recognition database, etc., capable of identifying individuals is misused or leaked, it is possible that their act and behavior histories will be retrieved in various ways, and besides, considering the possibility of future increase in accuracy of facial image and other databases and facial recognition systems and the widespread use of cheaper methods of storage in the cloud, etc., this may lead to significant violations of privacy in the future.

Therefore, the use of a system to cross-reference facial recognition data generated from facial image data of specific individuals obtained with their consent with specific persons seeking authentication for a match shall be allowed only in cases where there is a law expressly permitting such use, the consent is given voluntarily, and those who do not give consent may choose alternative means without suffering detriment, so that the privacy rights, etc., of citizens will not be violated unjustifiably, even if the system is aimed only at certain individuals who opt into such cross-referencing.

As a side note, it must be explicitly stipulated by law or regulation that, if a certain service is de facto unavailable unless consent is given, such consent is de facto coercion in the name of “voluntary” and shall not be permitted accordingly.[16]

[15] In theory, those who suspect that they may be registered erroneously should be allowed to request disclosure. However, in reality, the installer may possibly give the Glomar response, and therefore, in order to effectively guarantee their right to request correction, it must be ensured at least that inquiry will be made by a third-party body and the result will be disclosed promptly, as well as the reason for the registration will be disclosed to the data subject after a certain period of time.

[16] According to the reference material cited in footnote 12, the “Draft guidelines on processing of personal data through video devices” (July 10, 2019) of the European Data Protection Board provides that the facial recognition gates in an airport “must be installed … so that the biometric templates of non-consenting person will not be captured,” and the same shall apply to “on-sight” entry to concert venues, etc. Further, it is also provided that in cases where facial recognition technology is used for access management at offices, etc., alternative means to enter the office (presenting

Further, it should be required that a facial recognition system will not be applied to those who have not given consent, and the installer shall report to the Personal Information Protection Commission that it has installed and uses a facial recognition system so that the Commission can supervise as to whether the privacy of those who have given no consent is not violated.

(3) Systems for once-only cross-referencing without creating a facial recognition database that compare facial recognition data in storage media with specific individuals who opt into such cross-referencing

Risks similar to those discussed in (2) above will be posed also by systems to cross-reference the facial recognition data of specific individuals in storage media only once on the spot with those captured by security cameras, etc., to verify their identity if the facial recognition data are stored as a result of abuse. Thus, such use should be also limited to such cases as described in (2) above so that the privacy rights of citizens will not be violated unjustifiably.

5. Policy Measures That Should Be Immediately Discontinued

In light of the discussion under 4-(1) above, the police must immediately discontinue their investigations that are actually conducted using facial recognition systems aimed at a large number of unspecified persons without legislation that limits the scope of such investigations exclusively to investigation of serious organized crime.

Further, in light of the discussions under 4-(2) and 4-(3), at least the following activities must be discontinued:

(i) Use of facial recognition systems at the reception of medical institutions using individual number cards; and

(ii) Expanding the use of facial recognition data by linking the individual number card with the health insurance card, driver’s license, etc., thereby further increasing the scope of the use of facial recognition systems.

As for (i), considering the fact that there has been no inconvenience without even personal identification by photo so far and that the systems will be used in parallel with the current health insurance cards with no photo, there is no administrative necessity for such strict verification of identity to justify the use of facial recognition systems. Nonetheless, as discussed above, the government is strongly inducing medical institutions to introduce facial recognition card readers with a subsidy and even trying to abolish the paper insurance cards to integrate them with the individual number cards. By linking them with medical practice indispensable to protect the life and health of citizens, it will become de facto compulsory for them to use facial recognition systems, which will constitute a serious violation of privacy significantly deviating from the international

the employee ID card, etc.) must be provided, instead of forcing all the employees to use facial recognition.

human rights protection standard, and therefore it should not be implemented.

Further, as for (ii), by adding the functions of the health insurance card and driver’s license to the individual number card (and further abolishing the paper insurance cards to integrate it with the individual number cards), most citizens will be required in effect to carry their individual number card which is intended to be used in linkage with facial recognition systems. This will increase the risks of surveillance on citizens using facial recognition systems and therefore shall not be implemented.

In addition to such activities mentioned above, collecting and cross-referencing facial recognition data in public administration in general should not be permitted where verification by face photos is sufficient, because there is no need for such practice.

End.