Opinion Concerning the Legal Restrictions on Facial Recognition Systems

September 15, 2016

Japan Federation of Bar Associations

I. Summary of the Opinion

1. The opinion concerns the system whereby the police collect facial image data from an unspecified number of people nearby a crime scene, generate quantified data of characteristics to specify each individual (hereinafter referred to as "facial recognition data"), and conduct searches in a pre-generated database of facial recognition data of specific people (hereinafter referred to as a "facial recognition database"), which is used to match the identity of suspects or other persons. In regard to this system, it is the opinion of the JFBA that the nation should establish laws that incorporate the items listed below, amend relevant legislation and undertake similar measures to enact appropriate regulations, as well as recognize the guarantee of access rights for suspects, defendants and those in similar circumstances.

(1) Limitations on Usage Conditions

(i) Collection of facial image data recorded via security cameras or the like, for the purpose of criminal investigation by the police, should be conducted by court order (however, this would exclude facial image data from stores or other facilities, where such equipment has been legally installed in an area where the installer has authority).

(ii) Generating facial recognition data from images nearby a crime scene should be limited to those instances required for investigation of organized crime, where the crime infringes upon paramount public interests (hereinafter referred to as "serious organized crime"). In this case, facial recognition data that has been legally generated should be destroyed as soon as it is no longer required for said investigation.

(iii) Where use is permitted for facial recognition data generation from facial image data of suspects, previously convicted persons, or the like, whose facial image data is already in the legal possession of police, such use shall be limited to those with a previous conviction for serious organized crime.

(iv) Facial recognition data registered in the facial recognition database should be limited to those with prior convictions for serious organized crime. Furthermore, registration periods should be established for such data, and this data should be deleted immediately after the end of such registration period.

(v) Facial recognition database matching should be limited to such cases that require specific investigations for serious organized crime, and conditions for permitted methods should

be clearly predefistances.

(2) Monitoring by the Personal Information Protection Commission

The Personal Information Protection Commission should be able to check whether facial image data collection, facial recognition data generation, usage and disposal, compiling of facial recognition databases, registration to facial recognition databases, usage status of facial recognition databases, and data deletion or the like from the facial recognition databases, are conducted in an accurate and appropriate manner.

(3) Disclosure of Basic Information

The mechanisms and search accuracies of facial recognition systems should be periodically published.

(4) Rights of Suspects, Defendants and Those in Similar Circumstances

The facial recognition system can provide a means for claiming an alibi for those not connected to the facts of the crime. Requests by suspects, defendants, and those in similar circumstances for matching using the facial recognition system should be recognized. Furthermore, those erroneously registered in the facial recognition system should have recognized rights to request disclosure and deletion.

2. Until legislation incorporating the above is established, the Public Safety Commission should establish rules on facial recognition data that incorporate the measures set forth above, and should ensure that the application of this system is in accordance with such clearly stated rules. Prefectural police should also apply the system according to these rules.
3. From the perspective of preventing violation of privacy rights in applying the facial recognition system, the administration should verify that there is no collection and usage of facial image data at accuracies beyond what is required, and that there is no unnecessary generation and usage of facial recognition data. Further, the administration should pay close attention to this point moving forward.

   Specifically, existing facial image data held by the prefectural public safety commissions should not be provided to investigatory bodies without a court order, nor should further facial recognition data be generated.

II. Reasons for the Opinion

1. Introduction

Today, the use of security cameras installed by various installation entities (the police, business operators, shopping areas, individuals, etc.) is rapidly spreading nationwide, mainly in urban areas. Since it is considered in society that footage from such cameras contributes to a certain degree to early arrest of suspects, it is expected that areas with such camera installations will further expand and the density of cameras will increase. At the

same time, facial image data recorded by security cameras is becoming more sophisticated and their use in facial recognition systems for personal identification is also steadily expanding. This is likely to enhance their contribution in criminal investigations.

However, attention has to be paid to certain aspects of facial recognition systems. Since security cameras record the behavior of countless people without limitations regardless of whether a crime is committed or not, there are risks that portrait right and privacy rights of countless people may be violated depending on how they are managed, operated, and used. Moreover, facial recognition systems are equipped with a search function that allows identification of specific individuals out of a vast number of security camera images, which makes it possible to monitor the behavior of people, posing a further risk to privacy violations.

Alarmed by such a situation, the JFBA released the "Opinion Concerning the Legal Restrictions on Security Cameras" in 2012 (hereinafter referred to as the "2012 Opinion"), pointing out that the increase in "security cameras" which continuously photograph, video-record and distribute images of a large number of unspecified persons at an accuracy sufficient to identify individuals irrespective of whether a crime is committed cannot be ignored from the perspective of the guarantee of privacy rights, etc., and thus installation and operation of such security cameras need to be regulated by legislation that provides for certain standards and criteria therefor. However, there still exists no legal restrictions on the installation and operation of security cameras.

On the other hand, the technology of facial recognition systems is rapidly advancing and being put into practical use. Facial recognition systems generate facial recognition data by extracting characteristics such as the positional relationship of the eyes, ears, and nose, etc., of human faces extracted from still or motion images, and compare them with the facial recognition data registered in a facial recognition database to identify similarities. For example, a theme park has introduced a mechanism using facial recognition that allows annual pass holders who have registered their facial recognition data to be verified as a qualified visitor by just turning their face to the camera at the entrance without presenting their annual pass card that shows they are an annual pass holder. There is also an example where a facial recognition system using facial recognition data of shoplifters, etc., is introduced among multiple stores. There are risks of abuse in both cases, but particularly in the latter case, it could easily happen that individuals are monitored without their knowledge just because their facial recognition data are similar to those registered, which may lead to a violation of privacy rights, etc.

In light of such a situation, it can be said that prompt enactment of such law as proposed in the 2012 Opinion is becoming even more necessary.

2. Current Situation of Facial Recognition System Introduced by the Police

In FY2014, five prefectural police departments nationwide (the Metropolitan Police Department, Ibaraki Prefectural Police, Gunma Prefectural Police, Gifu Prefectural Police and Fukuoka Prefectural Police) experimentally introduced an apparatus to implement a facial recognition system (hereinafter referred to as "facial recognition apparatus").

The "portable facial image detection and matching apparatus" provided by the National Police Agency consists of a pre-generated facial recognition database and facial recognition/matching software (hereinafter referred to as "facial recognition software") incorporated in a notebook PC. An outline of the operation method of this system is as follows:

(1) A database of preregistered facial recognition data of ex-convicts of organized crime, etc., is created in advance;

(2) Footage from security cameras installed at and around a crime scene are collected;

(3) By using facial recognition software, human faces are extracted from the footage collected under (2) to generate facial recognition data, which will be instantly cross-referenced with (1) to determine at once whether any person similar to ex-convicts of organized crime, etc., was in the areas around a crime scene or surrounding areas at the time of a crime.

According to the specifications manual for bidding prepared by the National Police Agency, the system shall have the capabilities to "detect faces of 10 or more persons simultaneously," "detect faces of those wearing sunglasses or a face mask and faces not photographed from the front," "track the movements of the subjects," and "cross-reference with a database at 100,000 pieces of data within a second," and so on.

3. Study of the Fukuoka Bar Association

The results of the study on security cameras conducted independently by the Fukuoka Bar Association in 2014 revealed the following:

(1) The Fukuoka Prefectural Police limits the use of security cameras to cases where specific organized crime is suspected. The purpose of use is limited to investigation of organized crime, and security cameras are used by the Organized Crime Group Control Department (equivalent to the Organized Crime Control Division of other prefectural police departments).

(2) Security cameras are managed and operated according to the Fukuoka Prefectural Police Organized Crime Control Operational Regulations (internal regulations). The Regulations provide for the management of investigation materials and regulate the same to prevent information on organized crime groups from leaking.

Non-organized general crimes are not subjected to such investigation, but this is not

expressly stipulated in the Regulations.

(3) Footage from security cameras installed by private organizations can be collected in addition to footage from the security cameras installed by the Fukuoka Prefectural Police themselves.

(4) Individuals registered in a facial recognition database are limited as the system targets organized crime only.

However, there are problems with the operation described above. Namely, according to the results of the study, no operational guidelines in consideration of the sensitive nature of facial recognition data was prepared when the facial recognition apparatus was provided by the National Policy Agency; and the Fukuoka Prefectural Police has not prepared one either. Further, the abovementioned internal regulations used as the operational guidelines in the practice of such experimental operation stipulate general methods of management of information on organized crime groups, but do not contain provisions to specify crimes for which the facial recognition apparatus may be used or to limit the types of persons to be registered in the database subjected to detection and matching.

4. Severity of the Privacy Violation

(1) Nature of Facial Recognition Data as Privacy Information

A facial recognition system enables the police to conduct searches for the whereabouts of specific persons designated as targets by the police and track them using footage of security cameras once their facial recognition data are collected.

There are other means of verifying and proving the identity of individuals similar to facial recognition data, such as databases of fingerprints and DNA types, etc.

The Supreme Court judgment concerning the constitutionality of the fingerprinting system (December 15, 1995) held that “an individual’s fingerprint is a pattern on the individual’s fingertip, and the fingerprint itself does not represent any information on the individual’s private life or his/her inner mind, such as his/her personality, thoughts, beliefs and conscience. However, due to its nature, an individual’s fingerprint is unique throughout the world and it is permanent throughout the individual’s life, and there is the risk that the individual’s private life or privacy would be infringed depending on how his/her fingerprints taken by the authorities will be used. (snip) Since Article 13 of the Constitution can be construed to stipulate that people’s freedom in private life shall be protected from the exercise of state power, each individual, as one of his/her freedoms in private life, has the freedom of not being compelled to be fingerprinted without due cause, and it is against the purport of said Article and therefore impermissible for the state organ to compel any individual to be fingerprinted without just cause.” It can be

said that DNA types also have a nature similar to this.

Accordingly, it is not permitted today for the police to freely collect personal information on fingerprints and DNA types in their activities and such collection is restricted by the Rules of the National Public Safety Commission, but considering their high functionality for personal identification, restrictions by law are needed.

According to the specifications of the National Police Agency, the system shall be equipped with the "facial image search function" that enables "cross-referencing of facial detection images from real time footage with the registered facial images," so once facial recognition data are registered, it is thought to be possible, for instance, to automatically detect whether a specific person was present at a specific location by combining them with security cameras installed and managed by the National Police Agency and the prefectural police departments. Further, the system shall "be able to cross-reference all the facial detection images from the selected locations with the registered facial images," so it is thought to be possible to perform such automatic detection of the presence of specific persons at multiple locations.

Details as to the accuracy of such searches are unknown at present, but assuming that they are operated with high accuracy, they can be used not only for investigation of past cases but also to monitor the current behavior of specific persons regardless of whether an incident has occurred or not.

(2) Easiness of Generation of Facial Recognition Data

Facial recognition data of specific individuals can be automatically extracted by cross-referencing a facial recognition database with highly accurate facial images collected elsewhere using facial recognition software.

With the conventional security cameras, it was necessary for humans to directly watch moving images to check for the presence of suspects, and thus it was not so convenient in terms of achieving efficiency and accuracy when used for investigation. However, if the police have facial recognition software, facial recognition data can be generated by collecting data of security cameras widely from private organizations, etc., for investigation purposes as long as such images have accuracy of a certain level or higher, and a facial recognition database can be created by accumulating such data. The same is possible using footage of security cameras installed by the police themselves on the street or in facilities.

(3) Serious Violation of Privacy Rights

With respect to conventional security cameras, portrait right violation was at issue. But now that facial recognition software is put into practical use, it has become possible to search for and extract only such scenes with specific individuals from a vast amount

of footage of security cameras installed at diverse locations. By accumulating a large amount of such data, it is possible to monitor their daily activities for a long period of time, and therefore violation of privacy rights is becoming an issue.

Fingerprints or DNA samples alone are not capable of identifying individuals, and the risk is relatively low that they are collected without the person's consent. But this is not the case with facial recognition data. Just by walking in front of a highly accurate security camera, facial image data can be collected from which facial recognition data may be generated. Moreover, facial recognition data can be generated easily from facial recognition images of anyone by using facial recognition software, and if combined with successive time/date information and location information obtained from a large number of security cameras, it will be known even where and what the person was doing. Thus, unlike fingerprints and DNA samples, they pose a serious problem that they enable activities equivalent of peeping into the behavior and private life of specific persons.

Due to the development of digital data storage media and communication technology, it is becoming easier to store for a long time a large amount of video data of security cameras, which used to be difficult to accumulate, and to transmit them. In other words, citizens who are once subjected to surveillance by the police will be put in a situation where their long-term behavior history at a wide variety of locations in the past is searched, monitored, and used systematically by police departments throughout the country.

The Metropolitan Police Department has started to develop a "Automatic Three-dimensional Facial Shape Database Matching System" and an "Emergency Data Transmission System" utilizing footage of cameras installed by private organizations as a project based on the "Implementation Program 2009 for 'Tokyo 10 Years From Now'"[1] formulated by the Tokyo Metropolitan Government. If an unlimited facial recognition database is utilized for such project, it may become even possible for the police to search for, view and monitor the behavior history of numerous individuals.

5. Details of Legal Restrictions

(1) Necessity of Legal Restrictions

Considering that facial recognition data systems will be actively utilized as means of

[1] In 2006, The Tokyo Metropolitan Government formulated an urban strategy "Tokyo 10 Years From Now," which envisioned the appearance of Tokyo 10 years later when it was aiming at hosting the Olympic and Paralympic Games and set out the direction of its policies to achieve such a goal. It gave a picture of Tokyo achieving growth at a higher level for the near future not only in terms of urban infrastructure development but also in various fields including environment, safety, culture, tourism, industries, etc. To ensure the realization of the eight goals set in the "Tokyo 10 Years From Now" plan, an "implementation program" is formulated every fiscal year, and this "Implementation Program 2009 for 'Tokyo 10 Years From Now'" was formulated in FY2009.

investigations in the future, adequate measures need to be implemented to prevent abuses and protect privacy.

In the first place, comprehensively collecting images and generating facial recognition data of citizens unrelated to a criminal case limits their privacy rights, which are the basic rights guaranteed by the Constitution, and therefore, such activities must be positioned as compulsory investigation and shall not be implemented unless the same is permitted by law in advance as a means of investigation according to the principle of no compulsory dispositions without law (Article 197, Paragraph 1, Proviso of the Code of Criminal Procedure).

Restrictions on the abovementioned systems shall not be governed by internal rules or instructions/notifications of the police that tend to place too much emphasis on the convenience of investigations, but permissible conditions must be stipulated by law and enforced strictly.

(2) Collection of Footage from Security Cameras

As stated in the 2012 Opinion, footage of security cameras installed in the vicinity of a crime scene may be submitted voluntarily if such footage is related to a crime committed inside the facility, such as a store, etc., and is from cameras installed lawfully in areas over which the installer has authority, but otherwise footage shall be collected based on a search and seizure warrant.

(3) Restrictions on the Generation of Facial Recognition Data from Footage Collected in the Vicinity of a Crime Scene and their Disposal

It is within the scope of the purpose of collection under (2) to use facial image data collected lawfully in the vicinity of a crime scene as is, but if facial recognition data are generated additionally, the purpose is to cross-reference with other facial recognition data, and it needs to be noted that their infringing nature on privacy will be significantly higher. A facial recognition system would allow searches for the behavior history of citizens unrelated to a criminal case who happen to be at the site. So, if police departments nationwide introduce such a system focusing on convenience, the risk of privacy violation will significantly increase. Further, there is a possibility of malfunction in the process of generating or matching facial recognition data, which may cause a mistaken arrest. Taking these points into consideration, the use of facial recognition systems shall be limited to organized crime that may cause serious damage to legal interests (serious organized crime). Accordingly, the generation of facial recognition data from footage collected in the vicinity of a crime scene must be limited to cases where it is necessary for the investigation of serious organized crime.

Further, any facial recognition data that were once created but found to be

unnecessary for the investigation as they did not match or otherwise shall be immediately discarded. If facial image data are available, facial recognition data need not be stored as they can be generated from the facial image data.

(4) Registration in a Facial Recognition Database; Restrictions on the Generation of Facial Recognition Data and their Disposal

If facial recognition data are registered in a facial recognition database, it is very convenient for the investigating authority because it will enable police departments nationwide to generate facial recognition data from facial images collected in their investigation activities and cross-reference with facial recognition data registered in a facial recognition database.

However, this will mean to individuals whose facial recognition data are registered in a facial recognition database that they are constantly under surveillance as potential criminals and it will be checked whether they were at certain scenes of a crime taking place in various places of the country. This does not only conflict with their rights to privacy in the sense that their behavior history will be known to others, but also conflicts with their personal rights in the sense that they will always be treated as potential suspects once a crime has occurred.

Thus, facial recognition data to be registered in a facial recognition database should be limited to that of those who have been convicted of a serious organized crime.

In other words, generation of facial recognition data from facial image data collected lawfully (Article 218, Paragraph 3 of the Code of Criminal Procedure, etc.) by the police, instead of using facial image data as is, should be permitted only in cases where they are used in a facial recognition database, and the data subjects must be limited to ex-convicts of serious organized crime.

Even in such cases, it will infringe on their personal rights and therefore is not reasonable to have such data registered for an indefinite period of time and used in criminal investigations for their entire life, as this means that they will continue to be treated as dangerous persons who are likely to reoffend at all times. In the “Opinion on the National Police Agency’s DNA Database System” (dated December 21, 2007), the JFBA called for consideration of limiting the registration/retention period of suspects’ DNA profile information to five to ten years. A similar limitation must be stipulated also for the registration period of facial recognition database, and the data shall be discarded upon expiration of such period.

(5) Cross-referencing with a Facial Recognition Database

Further, even when data are used for cross-referencing using a facial recognition database for investigation purposes, such use must be limited to cases where there is a

need for specific investigation of a serious organized crime to strike a balance with the protection of privacy rights, etc., and conditions must be stipulated by law as to permitted methods of their use.

(6) Supervision by the Personal Information Protection Commission

The Personal Information Protection Commission established under the Act on the Protection of Personal Information assumes the duties of ensuring the proper handling of personal information in order to protect an individual's rights and interests while considering the utility of personal information and has the authority to supervise and give guidance and advice and so on (Article 51 of the Act on the Protection of Personal Information). Currently, its authority is limited to the scope of the private sector and the individual number system, but the relevant laws and regulations should be amended to expand it to cover the handling of personal information for public administrative agency purposes or by the police so that it can check whether the collection of facial image data, the generation, acquisition, use and disposal of facial recognition data, the creation, registration and use of a facial recognition database and the deletion of data from it, etc., are appropriately conducted.

As a side note, members of the prefectural public safety commissions do not have expertise in the protection of personal information, and it is stipulated that general affairs of the public safety commissions shall be handled at the Metropolitan Police Department or the relevant prefectural police headquarters (Article 44 of the Police Act). Thus, the public safety commissions are not sufficiently independent from the Metropolitan Police Department and the prefectural police headquarters, and therefore not suitable as a supervisory body.

(7) Disclosure of Basic Information

As discussed above, a facial recognition system is currently utilized experimentally by some police departments and such application may be expanded to criminal investigations, but little information is disclosed regarding its mechanism and search accuracy. If it is overestimated despite that its actual accuracy is not sufficiently high, the risks of mistaken arrests and false charges will increase. Therefore, the basic information on the system should be disclosed on a regular basis and any changes must be clarified.

(8) Rights of Suspects/Defendants, etc.

A facial recognition system can provide a means for claiming an alibi for those not related to crimes, if used to determine that facial recognition data generated from the facial image of a criminal captured in the footage from the crime scene do not match the facial recognition data generated from the facial images of those other than the criminal.

Thus, matching by a facial recognition system must be allowed at the request of defense councils, suspects, defendants, persons requesting a retrial, etc.

Further, those who have been erroneously registered in a facial recognition database must be granted a right to request disclosure of personal information to inquire whether their facial recognition data are registered in such database. As a prerequisite, a right to request deletion of erroneously registered facial recognition data should be granted.

6. Operation Pending the Enactment of Legislation

As of today, such legislation as discussed above is yet to be enacted, but the facial recognition apparatus is operated at the aforesaid five prefectural police departments. Sufficient measures of privacy protection must be taken in such operation by the police as well, focusing on the need to protect facial recognition data.

At least, until a mechanism of legal restrictions is put in place, the National Public Safety Commission should establish regulations concerning facial recognition data providing for the abovementioned content and make an effort to ensure that the system will be operated in compliance with the rules stipulated in advance. The relevant prefectural police department should also operate the systems according to such rules.

7. Public administrative agencies shall neither collect or use facial image data at accuracies beyond what is required nor generate and use facial recognition data where unnecessary.

Apart from the facial recognition system, there already exist a large amount of facial image data of citizens collected and held by public administrative agencies.

For example, from 1994 and onward, facial image data are collected and stored as digital data by the prefectural public safety commissions when a driver's license is created or renewed. Depending on the accuracy of such data, it is technically possible to use the data in combination with a facial recognition system, but since such face photo data are collected for the purpose of creating driver's license cards that are used to determine whether a person driving a car has a license to drive, it should not be permitted to submit such facial image data to the investigating authority without a warrant issued by a court judge or to generate facial recognition data from the same.

Moreover, for any collection and use of facial image data that are accurate enough to enable generation of facial recognition data, consideration is required as to whether the same are absolutely necessary to achieve the administrative purpose.

This shall apply where other public administrative agencies or municipal governments collect or have already collected facial image data based on their administrative necessity. Thus, public administrative agencies must examine whether they collect and use facial image data at accuracies beyond what is required or generate and use facial recognition data where unnecessary, and due caution must be exercised in this regard in the future as

well.

8. Conclusion

As discussed above, the JFBA believes that legislation incorporating the content pointed out in the Summary of the Opinion must be enacted to restrict the operation of facial recognition systems.

End.