



HAL
open science

The Use of Live Facial Recognition Technology by Private Entities in Public Places: A Study of Recent Case in Japan

Aimi Ozaki

► **To cite this version:**

Aimi Ozaki. The Use of Live Facial Recognition Technology by Private Entities in Public Places: A Study of Recent Case in Japan. 15th IFIP International Conference on Human Choice and Computers (HCC), Sep 2022, Tokyo, Japan. pp.27-35, 10.1007/978-3-031-15688-5_3. hal-04395452

HAL Id: hal-04395452

<https://inria.hal.science/hal-04395452v1>

Submitted on 15 Jan 2024

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



Distributed under a Creative Commons Attribution 4.0 International License



This document is the original author manuscript of a paper submitted to an IFIP conference proceedings or other IFIP publication by Springer Nature. As such, there may be some differences in the official published version of the paper. Such differences, if any, are usually due to reformatting during preparation for publication or minor corrections made by the author(s) during final proofreading of the publication manuscript.

The Use of Live Facial Recognition Technology by private entities in public places: A Study of Recent Case in Japan

Aimi Ozaki ¹[0000-0002-7619-8514]

¹ Faculty of Social Sciences, Kyorin University, Tokyo, Japan
ai-ozaki@ks.kyorin-u.ac.jp

Abstract. In July 2021, East Japan Railway Company introduced a face recognition function to some of its security cameras. However, the company was criticized by society for not fully disclosing its detailed operation policy, and later withdrew some of its operations. Recently, Japan has seen an increase in the number of indiscriminate killings and injuries on trains, and there are growing calls for the need for AI-based countermeasures against suspicious persons. Therefore, why did East Japan Railway Company receive social criticism? In this paper, I would like to clarify the reasons and explore the ideal form of legal regulation for facial recognition systems used by private entities.

Keywords: Live Facial Recognition, Privacy, Personal Data, Fairness

1 Current situation in Japan

1.1 Use of facial recognition automated gates and its guidebook

As it stands in 2022, guidelines for face recognition technology have been established in Japan for some use cases. For example, in March 2020, the Ministry of Land, Infrastructure, Transport and Tourism (MLIT) published a guideline on the handling of personal data such as passenger facial images, passport information, and boarding information. (This guideline is called the "Guidebook on the Handling of Personal Data in One ID Services Using Face Recognition Technology at Airports [1].) Narita Airport and Haneda Airport are currently preparing to introduce the "One ID Service," a boarding process that uses facial recognition technology. However, there has been strong social criticism of the acquisition of facial image information. This is because facial image information is an identifier that is highly immutable and can be easily acquired without the person's will, and thus has a strong tracking function. Therefore, this guidebook outlines three matters that should be considered when handling personal information at the time of introducing the "One ID Service". The first is prior notification and public announcement, the second is obtaining passenger consent, and the third is establishing a mechanism for receiving complaints and consultations regarding personal information from passengers. The following three points should be considered in the operation of the One ID service. First, the use of personal data should be limited to the boarding process; second, facial recognition should be used only for passengers

who wish to use it, and the existing procedures should remain in place; and third, in principle, personal data should be deleted within 24 hours, and audits should be conducted periodically.

1.2 Facial recognition system provided by East Japan Railway Company

In Japan, there are various examples of the use of face recognition technology, including in fields other than airports. In July 2021, East Japan Railway Company announced that it would introduce a new security method using security cameras at some stations in the Tokyo metropolitan area during the Tokyo Olympics and Paralympics [2].

The security cameras are equipped with behavior analysis technology and face recognition technology to detect suspicious persons and objects. When the camera detects a suspicious person or object, the security center will report the incident to the security guards, who will respond promptly. Furthermore, in the event of an emergency situation such as a terrorist attack, East Japan Railway Company will transmit the images from the security cameras to the police through the emergency image transmission system [3], and will work with the police to deal with the situation.

The emergency image transmission system consists of a 3D face shape database conversion system and an automatic matching system. The 3D face shape database conversion system (1) estimates 3D face shape data from photographic images, (2) creates 2D face image data from various angles from 3D face shape data, and (3) registers the created face image data to the MPD server. The automatic matching system (1) transmits the face image data extracted from the security camera images to the MPD server, (2) matches the transmitted face image data with the data registered in the MPD server, and (3) stores the transmitted face image data in the MPD server. (3) If the transmitted face image data and the data registered in the MPD server match, the police station is notified. (4) If the transmitted face image data and the data registered in the MPD server do not match, the transmitted face image data will be automatically deleted.

1.3 Press reports

In August 2021, through press reports, it became clear that East Japan Railway Company was targeting not only (1) suspicious persons, but also (2) persons who had been released or paroled after serving time in prison for major crimes related to the company, and (3) persons wanted by the police [4]. According to subsequent media reports, East Japan Railway Company was planning to receive information on people released from prison from the standpoint of victims, based on the "Victim Notification System," which informs victims of incidents of their release or parole [5]. In addition, stickers stating "face recognition camera in operation" were placed near some ticket gates, although East Japan Railway Company replied to the newspaper that it could not reveal the detailed location and number of security cameras installed.

This report caused many opinions to be sent to East Japan Railway Company. Some of them were rather criticized. According to the report, some people were worried that the symptoms of their chronic illnesses might make them look suspicious. East Japan Railway Company's press release stated that the system would be implemented "during

the Tokyo 2020 Games," so some people thought it was understandable if the system was implemented during the Olympics, although they did not expect it to continue after the Games closed. Later, investigative reports revealed that "serious incidents" were assumed to be terrorist incidents in which passengers were targeted, and not sex crimes or theft. Furthermore, East Japan Railway Company did not disclose how users could request for disclosure or deletion, and did not disclose the retention period of the video images taken of passengers. In September 2021, East Japan Railway Company suspended the detection of people released from prisons because "social consensus has not yet been reached. However, East Japan Railway Company appears to have continued to detect (1) suspicious persons and (2) persons wanted by the police.

An East Japan Railway executive commented in an interview that the measures were taken out of a single-minded desire to protect the safety of passengers. In Japan, there have been many sex crimes committed on trains, and recently, there has been an increase in indiscriminate killings on trains. Against this situation, there are increasing calls for the need for AI-based countermeasures against suspicious persons. Therefore, why has East Japan Railway Company been socially criticized? In this paper, I would like to clarify the reasons and explore the appropriate form of legal regulation for face recognition systems used by private entities.

2 Guidelines of the Personal Information Protection Commission and East Japan Railway Company's measures

East Japan Railway Company explained that they had consulted with the Personal Information Protection Commission and had taken measures in compliance with the law. The Personal Information Protection Commission also commented, "Act on the Protection of Personal Information strikes a balance between protection and use, and East Japan Railway Company's case is not out of balance if the use is limited to the purpose of crime prevention". However, in September 2021, the Personal Information Protection Commission revised the "QUESTIONS AND ANSWERS on the "Guidelines for the Act on the Protection of Personal Information" and the "Handling of Personal Data Leaks and Other Incidents" [6]. In the following, after examining the contents of the revised QUESTIONS AND ANSWERS on the Act on the Protection of Personal Information, it will be discussed whether East Japan Railway Company's measures can be considered to be in line with this QUESTIONS AND ANSWERS.

2.1 Questions and Answers on Act on the Protection of Personal Information

Under the Act on the Protection of Personal Information, the taking and recording of camera images that can be used to identify individuals constitutes the acquisition of personal information. Therefore, it is necessary for the business operator to disclose the purpose of use of personal information to the user in advance, or to notify or disclose the purpose of use of personal information promptly after the acquisition of personal information. Previously, the Personal Information Protection Commission explained

that when a business operator takes a picture using a security camera only for the purpose of crime prevention, the business operator does not need to notify users of the purpose of use of personal information or make it public because the purpose of use is clear. (Article 18, Paragraph 4, Item 4 of the Act on the Protection of Personal Information)

However, in September 2021, the Personal Information Protection Commission changed its previous interpretation. The following is the new interpretation of the Personal Information Protection Commission.

The Personal Information Protection Commission answers the assumed question, "What precautions should be taken when a business operator intends to introduce a facial recognition system for crime prevention purposes, limiting the target to criminal acts such as theft?" The following is an answer to the question. "If a business operator builds a personal information database by systematically composing camera images and face recognition data that can be used to identify a user, the information including individual camera images and face recognition data will fall under the category of personal data. Therefore, in this case, the business operator needs to handle the information appropriately in accordance with the Personal Information Protection Law. In addition, when a business operator intends to use personal data including face recognition data by installing a face recognition system for the purpose of crime prevention, limiting the target to criminal acts such as theft, the business operator must register the data with the face recognition system to the minimum extent necessary to achieve the specified purpose of use, and must keep the personal data. It is necessary to maintain accurate and up-to-date content. Specifically, business operators should set up internal rules on what criteria should be used for registration in the database. In addition, service providers should establish a system whereby registration to the facial recognition system is made only when a crime is objectively confirmed, and the necessity and accuracy of the registration is confirmed by a responsible person within the service provider. Furthermore, when businesses use security cameras to acquire camera images and extract face recognition data from them for use, the users themselves cannot reasonably predict or assume that such handling will take place. In addition, facial recognition data is personal information that can also be used for marketing purposes. Therefore, businesses shall specify the purpose of use so that users can predict and assume that camera images and face recognition data using face recognition technology will be handled for security purposes. In addition, the business operator must notify the user of the purpose of use of the acquired data, either publicly in advance or promptly after acquiring the data. Business operators are required to post at the entrance or at the installation site, etc., that the security cameras are in operation, and to take measures to make it easily recognizable to users that their personal information is being obtained by the security cameras. In addition, the entity that acquires the camera images, the contents of the camera images, the purpose of use of the camera images and face recognition data, and the contact information for inquiries must be clearly indicated at the entrance of the store or at the installation site, or the URL or QR code of a website containing such information must be shown so that the user himself/herself can check it."

2.2 Measures taken by East Japan Railway Company

East Japan Railway Company's measures in this case appear to be inadequate. According to media reports, East Japan Railway Company only placed a sticker (3.5 cm in length and 27 cm in width) near some ticket gates that read "Face Recognition Camera in Operation. This is not a sufficient measure to make it easy for users to recognize that their personal information is being obtained.

In addition, East Japan Railway Company's website states in its "Basic Policy on the Handling of Personal Information" that "Images obtained from security cameras installed in stations will be registered in a face recognition database created by the Company, to the minimum extent necessary, only when necessary to ensure security in stations and trains. It will be used for crime prevention and security in stations and trains. This was the only wording in the document. Therefore, it cannot be concluded that the purpose of use of the facial recognition data was clearly stated.

2.3 Special care-required personal information

Information that a person has served time in prison is considered "Special care-required personal information" under the Act on the Protection of Personal Information. "Special care-required personal information" in Act on the Protection of Personal Information means personal information comprising a principal's race, creed, social status, medical history, criminal record, fact of having suffered damage by a crime, or other descriptions etc. prescribed by cabinet order as those of which the handling requires special care so as not to cause unfair discrimination, prejudice or other disadvantages to the principal. (Article 2, Paragraph 3 of the Act on the Protection of Personal Information.)

3 Discussion in Japan

The cause of this issue is that East Japan Railway Company started the system without disclosing the details of the system, even though a "social consensus" on the use of the facial recognition system in public spaces had not been formed.

For example, Prof. Makoto Ibusuki of Seijo University, an expert in criminal procedure law pointed out that detecting facial information of released prisoners and parolees is inconsistent with the direction of Act for the Prevention of Recidivism, which encourages the prevention of recidivism and rehabilitation of those who have committed crimes [7]. Furthermore, Professor Ibusuki suggests that we must thoroughly debate whether we really need such a discriminatory surveillance system, because identifying people with criminal records in public spaces could become a modern version of "digital tattooing.

In response to such criticism, East Japan Railway Company has stopped detecting people released from prisons. However, this does not mean that there are no problems with East Japan Railway Company's ongoing methods of detecting suspicious persons

and those wanted by the police. For example, in the United States, it has been suggested that whether stored, real-time, or through third-party image searches, building a system with the potential to arbitrarily scan and identify individuals without individualized suspicion and to discover personal information about their location, interests, or activities should simply be banned by law [8]. In the following, I will introduce the discussion in Japan and suggest what the legal regulations for facial recognition systems used by private entities ought to be.

3.1 Requirements for private entities to use facial recognition systems in public spaces

Professor Ibusuki states that there are three requirements for businesses to use facial recognition systems in public spaces.

The first is the consent and approval process at the facial information collection stage. Contrary to fingerprints and DNA, facial information can be easily collected without the user's consent. Consent and approval processes are necessary not only for identifying facial images in public spaces, but also for collecting facial information in the original data. Second, the purpose and use of facial recognition technology should be made public and evaluated by a third party. As long as businesses are not accountable, the use of such technologies will not be allowed. The third is to establish an independent, neutral, and technologically savvy nationwide review body that will check the use of facial recognition technology in advance and verify the actual operation.

3.2 Opinion by Japan Federation of Bar Association

The Japan Federation of Bar Associations (“JFBA”) compiled an opinion paper, “Opinion on Statutory Regulations on the Use of Facial Recognition Systems by Public and Private Sector Organizations and Incorporated Administrative Agencies,” dated September 16, 2021, and submitted it on September 21, 2021 to the Commissioner General of the National Police Agency; the Superintendent General of the Metropolitan Police Department; the Chiefs of Prefectural Police Headquarters; the Minister of Internal Affairs and Communications; the Minister of Health, Labour and Welfare; the Chairperson of the Personal Information Protection Commission; prefectural governors; and mayors of the cities designated by Cabinet Order [9].

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

Subsequently, the Japan Federation of Bar Associations issued a Chairman's Statement requiring the suspension of the use of facial recognition systems by railroad operators. The contents of the Chairman's Statement are as follows [10].

The inside of a station is a space managed by a railroad operator. Nevertheless, station premises are extremely public spaces that are used by an unspecified number of people on a daily basis and can be considered essential to everyone's life. If it is a store, users can choose another store that does not introduce the facial recognition system. However, in the case of public transportation, it is not necessarily possible for users to make other choices. The introduction of a face recognition system by a railroad operator may become a de facto compulsion for users, which would seriously infringe on their right to privacy.

The detection of a wanted suspect by a railroad operator is not the same as a station attendant who happens to find a wanted criminal, even if it is for the purpose of cooperation in an investigation by the private sector. It is a surveillance of all people in many stations. In a sense, it is as if the railroad operators are systematically and continuously operating a wanted criminal detection device 24 hours a day. In effect, this is equivalent to the police setting up a facial recognition system and using it without any legal basis or court warrant, and it is a violation of the statutory principle of compulsory punishment. (Proviso of Article 197, Paragraph 1, of the Code of Criminal Procedure)

Furthermore, since the definition of "suspicious person" is ambiguous, there is a risk that private businesses will operate arbitrarily based on subjective judgment criteria. In other words, there is a risk that people will be regarded as suspicious without their knowledge, and their baggage will be searched or the police will be called. This is a threat to a free civil society.

Currently, it is possible to search, match, and utilize facial image data in real time. Once the facial image data is registered in a database, the person's behavior can be accurately tracked back to the past and then continuously monitored. In the European Union, the use of facial recognition systems for unspecified persons in public places is prohibited in principle. In the United States, state laws and regulations are in progress. These are based on the same awareness of the problem.

In Japan as well, the use of facial recognition systems should be based on strict legal provisions with careful consideration of necessity and reasonableness. In addition, it is difficult to easily justify the use of facial recognition systems in highly public spaces, even by legislation, if the users do not give their consent. Therefore, the use of facial recognition systems by railroad operators should be stopped immediately.

3.3 Conclusion

Professor Ibusuki's view is based on movements in developed countries that have already adopted face recognition systems, and extracts the requirements for businesses to use facial recognition technology in public spaces in Japan. Therefore, the three requirements are at a level of detail comparable to recommendations in other countries. However, as pointed out by Professor Ibusuki, obtaining consent as a legal measure does not work well because of the ease with which biometric information can be collected. When businesses use facial recognition technology, it will be necessary to discuss among stakeholders whether the consent model should be maintained or whether an alternative to the consent model should be designed.

The views of the Japan Federation of Bar Associations are more stringent. They have issued a chairman's statement stating that railroad operators should immediately stop using facial recognition systems because they do not comply with the above conditions. However, with the increasing number of indiscriminate killings on trains in Japan, there are growing calls for the need for AI-based measures against suspicious persons. In such a situation, abolishing suspicious person detection systems may go against social demands.

In December 2021, the Personal Information Protection Commission established a study group to discuss the appropriate use of camera images for crime prevention in public spaces. It is anticipated that legal regulations for facial recognition systems will be advanced in Japan in the future. In this situation, legal regulations or guidelines should be formulated for each type and use case of facial recognition technology after establishing a basic framework.

In the first place, the reason behind the social criticism of East Japan Railway Company is that there are deep-rooted concerns that the facial recognition system will infringe on the privacy of users, and furthermore, that it will lead to a surveillance society and infringe on freedom of expression. In addition to these concerns, it has been pointed out that the facial recognition system has the potential to promote prejudice and discrimination. Actually, in this case of East Japan Railway Company, the initial target of detection was persons who had been released or paroled from prison, which could have resulted in social exclusion for persons who had completed atoning for their crimes. This kind of discriminatory operation must be prevented.

In addition, East Japan Railway Company's ongoing method of detecting suspicious persons and those wanted by the police is not without its problems. The face recognition system introduced by East Japan Railway Company in this case is live facial recognition. The Information Commissioner's Office (ICO) provides the following description of live facial recognition. "It is directed towards everyone in a particular area rather than specific individuals. It has the ability to capture the biometric data of all individuals passing within range of the camera automatically and indiscriminately. Their data is collected in real-time and potentially on a mass scale. There is often a lack of awareness, choice or control for the individual in this process" [11].

For this reason, the EU has proposed a draft regulation that would, in principle, prohibit live facial recognition in public spaces for law enforcement purposes, except in exceptional cases. The exceptional cases are the search for missing children, the

prevention of imminent terrorist threats, and the arrest of suspects of serious crimes. The exceptional use of live facial recognition would require authorization by a judicial or other independent body. Restrictions are also placed on the databases to be used and the time and place coverage.

East Japan Railway Company states that the emergency image transmission system will only be activated in the event of an emergency situation such as terrorism, but the conditions for its activation are unclear. In addition, in order to implement the emergency image transmission system, cooperation with investigative agencies is essential. However, it is also unclear how information is shared between railroad operators and investigative agencies. This is because the Act on the Protection of Personal Information considers that the consent of the user himself/herself is not required when an investigative agency requests a business operator to provide information about the user for the purpose of investigation [12].

In the U.K., where live facial recognition is increasingly regulated, The ICO have published a Commissioner's Opinion on the use of LFR in public places by private companies. The ICO requires controllers that they must be transparent with the public about who is processing their personal data and for what purpose and they must be communicated clearly, including through any signage, other communications and associated privacy information.

In Japan as well, when operators share information with investigative agencies, they will need to maintain the transparency described above. This is the first step for businesses to obtain a "social consensus" to use facial recognition systems in public spaces. In designing future legal regulations for facial recognition systems in public spaces for the purpose of crime prevention, it is essential to provide guidelines on how information should be shared with investigative agencies.

References

1. Ministry of Land, Infrastructure, Transport and Tourism (MLIT), Guidebook on the Handling of Personal Data in One ID Service Using Face Recognition Technology at Airports. <https://www.mlit.go.jp/report/press/content/001332966.pdf>
2. East Japan Railway Company, Efforts to Improve Railway Security for the Tokyo 2020 Olympic and Paralympic Games. https://www.EastJapanRailwayCompany.co.jp/press/2021/20210706_ho02.pdf
3. Tokyo Metropolitan Government, "A New Tokyo" Created by Citizens First: An Action Plan for 2020. https://www.kantei.go.jp/jp/singi/tokyo2020_suishin_honbu/kan-jikai/dai7/sankou.pdf
4. Masako WAKAE, More transparency needed with facial recognition technology, The Japan News, Sep 1, 2021 at 3.
5. East Japan Railway Company's facial recognition watch list attracts scrutiny / Targeted individuals set to include ex-prisoners, The Japan News, Sep 22, 2021 at 1.

6. The Personal Information Protection Commission, QUESTIONS AND ANSWERS on the "Guidelines for the Act on the Protection of Personal Information" and the "Handling of Personal Data Leaks and Other Incidents."
https://www.ppc.go.jp/personalinfo/faq/2009_APPI_QA/
7. Makoto IBUSUKI, "Identifying the faces of all passengers with surveillance cameras," What was wrong with East Japan Railway Company's system for detecting people leaving prison?, President Online, Oct 29, 2021.
<https://president.jp/articles/-/51210?page=1>
8. Andrew Guthrie Ferguson, Facial Recognition and the Fourth Amendment, 105 MINN. L. REV. 1105 (2021) 1197-1198.
9. Japan Federation of Bar Associations, Opinion on Statutory Regulations on the Use of Facial Recognition Systems by Public and Private Sector Organizations and Incorporated Administrative Agencies.
<https://www.nichibenren.or.jp/en/document/opinionpapers/210916.html>
10. Japan Federation of Bar Associations, Chairman's Statement Calling for the Discontinuation of the Use of Facial Recognition Systems by Railroad Operators.
<https://www.nichibenren.or.jp/document/statement/year/2021/211125.html>
11. The Information Commissioner's Office, Information Commissioner's Opinion: The use of live facial recognition technology in public places.
<https://ico.org.uk/media/2619985/ico-opinion-the-use-of-lfr-in-public-places-20210618.pdf>
12. Taro KOMUKAI, Privacy protection in the criminal investigations on the personal data held by third parties, Journal of Information and Communications Policy Vol.4 No.1, at 67.
https://www.soumu.go.jp/main_content/000719095.pdf