Privacy Measures of Biometrics Businesses

SAMESHIMA Shigeru

Abstract

The Japanese Act on the Protection of Personal Information updated and enforced in 2017 makes it clear that individual identification code such as DNA, facial feature quantities and iris information are to be classified under personal information. Similarly, mainly in Europe and North America, respects for of human rights and privacy are needed for human surveillance and tracking technologies at a worldwide scale.
In this paper the author reviews the privacy measures of the biometrics businesses for which careful discussions are required, as based on efforts currently being applied by NEC.

Keywords
privacy, human rights, biometrics, facial recognition, transparency, Privacy by Design, Human Rights by Design

1. Introduction

Biometric authentications such as for facial recognition are increasing opportunities for usage diversity, from the unlocking of smart devices to immigration control procedures. NEC has also implemented various types of introductions at airports and in retail industries, as described in this special issue. However, as some case studies show their issues by employing biometric authentication, it is important to give great consideration to human rights, privacy, etc. when the technology is applied to our society.

In this paper, section 2 reports on the legal regulations that govern biometric information in Japan, the EU and the USA, section 3 introduces the human rights and privacy cases that have posed issues in the past. Section 4 describes efforts being made regarding human rights and privacy considerations and the final section provides a short conclusion to the paper.

2. Outline of Legal Regulations on Biometric Information

The regulations guidelines related to the biometric businesses cover a wide range of domains when the guidelines for each business type are discussed, therefore, this paper gives only the outlines of legal regulations related to biometric information in Japan, the EU and the USA (**Table**). For recent trends, it is required

Table Definitions of biometric information in different countries (Outline).

	Biometric information definitions (Outlines)
Japan	Codes obtained by converting the features of some part of the human body for use by computers -> DNA, face, iris, voiceprint, appearance of walking, venous characteristics of hands or fingers, finger or palm prints
EU	Personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person (Examples) Facial images, dactyloscopy data, etc. * A Separate definition is given for the genetic data.
USA	• No federal law giving the definition • Only three state laws (Illinois, Texas, and Washington) give the definitions. · Retina/iris scan, fingerprint, voiceprint, or record of hand or face geometry (Texas Business and Commerce Code § 503.001)

to clarify the biometric information subject to the legal regulations and to provide robust management and operational procedures[1].

2.1 Japan

The Japanese Act on the Protection of Personal Information, as updated and enforced in 2017 makes it clear that the individual identification code that belong to such personal information are those such as: DNA, face feature quantities, the iris, voiceprints, physical appearance when walking and intravenous shape of hands or fingers, as well as for finger or palm prints. Consequently, when one wants to obtain face feature quantitative data using a camera, it is mandatory to announce the purpose of its use publicly or to notify the subject. Moreover, should any breaches of the face feature quantitative data occur, the Personal Information Protection Commission and relevant authorities should be provided with details of the breach.

2.2 EU

The EU General Data Protection Regulation (GDPR) that became enforceable at the beginning of May 2018 gives a definition of the biometric data, makes it clear that it is the subject of regulation and also requests a data protection impact assessment of biometric data handling. If a breach of biometric data occurs a competent supervisory authority shall be provided with details of the breach within 72 hours after having become aware of it. Infringement of this regulation shall be subject to administrative fines up to €10 million or, in the case of an undertaking, up to 2% of total worldwide annual turnover, whichever is higher.

2.3 USA

There is no federal law giving direct definition of biometric information and only three states (Illinois, Texas and Washington) offer a direct definition of biometric information and regulate it under their state laws. On the other hand, for the facial recognition, federal institutions announce a large number of best practices and guidelines backed by the progress and dissemination of the technology[2]. Considering the presence of such a large number of biometric businesses in the USA, it is regarded that their independent efforts may be expected.

3. Human Rights and Privacy Issues

Even if a biometric business is run by observing legal regulations, there may be cases in which human rights, including privacy rights become issues. This is because human rights are not simply as prescribed in national constitutions but are defined as "the rights naturally possessed by humans based only on the fact that they are humans"[3] and that the concept varies depending on age, country and region.

Particularly, as the information obtained with sensor devices including cameras and microphones does not need contact for acquisition and its acquisition is easily achieved it may often become a source of issues from

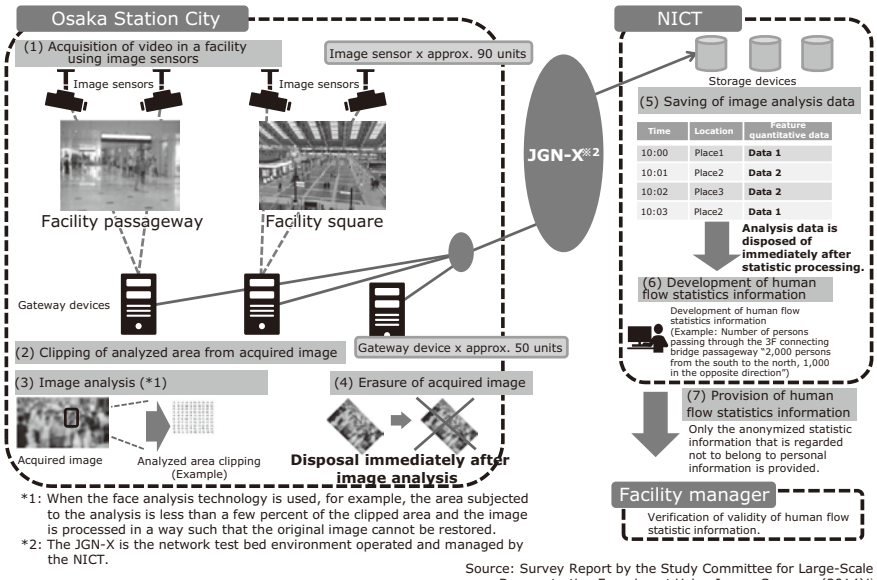

Fig. 1 Outline of the demonstration experiment.

the viewpoint of human rights. The rest of this section deals with cases of problems associated with cameras.

3.1 Lack of privacy considerations in the planned experiment for people-flow analysis in the Station Building (Japan)

In 2014, the National Institute of Information and Communications Technology (NICT) planned a demonstration experiment to identify human flow and its retention by installing 92 cameras in the Osaka Station City area and by shooting passersby in order to verify the usability of the information as a part of the safety measures applied after a disaster (**Fig. 1**). This plan was however postponed due to the insecurity related issues to privacy violations expressed by citizens and influential individuals.

Subsequently, a third-party panel was organized by external influential individuals and a proposal was made to the NICT, which is the implementing body. The proposal pointed out that the demonstration experiment itself cannot be regarded as illegal but that the accountability is inadequate in terms of the measures available for obtaining consent on the significance of the demonstration and on reducing the anxiety of citizens[4].

3.2 Criticism of the use of facial recognition systems by police (USA)

In the USA, two dozen of the civil rights organizations have requested discontinuation of sale of the facial recognition system (Amazon Rekognition) that Amazon.com, Inc. supplied to the police (e.g. Orland in Florida), claiming that it is designed to facilitate abuse by governments. This request points out that facial recognition software poses important threats (such as mistaken arrests) to minorities, which include colored persons and immigrants, because its false recognition rate is higher for colored persons than for white persons.

4. Human Rights and Privacy Measures

Then, what kind of approach should a company take against matters related to human rights and privacy issues? Among the various approaches that may be possible, the following section examines specific cases from the viewpoints of the considerations, transparencies of products and services.

4.1 Products and services with human rights and privacy considerations

The considerations inherent in products and services first come to mind. These consist of considering the human rights and privacy issues by examining the function of each product/service and the means and end of its implementation.

For instance, when human flow and congestion in a busy district are analyzed in order to examine the measures to be taken in urban development, it is not necessary to identify each and every passerby. In such a case, the process of avoiding personal identifications may be applicable, by pixelizing or defocusing the faces of those passersby captured by the cameras or by replacing actual persons with human-shaped likenesses. However, the pixelization and defocusing could sometimes allow certain identifications, for example of a couple such as a parent and child or a person in a wheelchair, from its silhouette shape. From this viewpoint, the replacement by human-shaped likenesses is applied without exception to the passersby, so that identifications from the silhouette shapes becomes impossible. For instance, in the case of the purpose for the visualization of congestion in a certain space, the likeness replacement process may be regarded as giving a higher privacy consideration.

Another possible analysis method is to generate the passerby attribute information that cannot lead to their identifications (age groups, gender, etc.) from the camera image and to destroy the original image enabling personal identifications immediately after the generation. This method enables analysis based on the estimated information such as age groups and genders of passersby, so that it may be used when the purpose is to analyze the activation of a busy district (**Fig. 2**)[5].

4.2 Transparency

It is additionally important to declare sincere explanations of the purpose of the project and the processing of the acquired personal data, from the viewpoints of actual citizens.

Aiming at a system that can predict hazardous con-

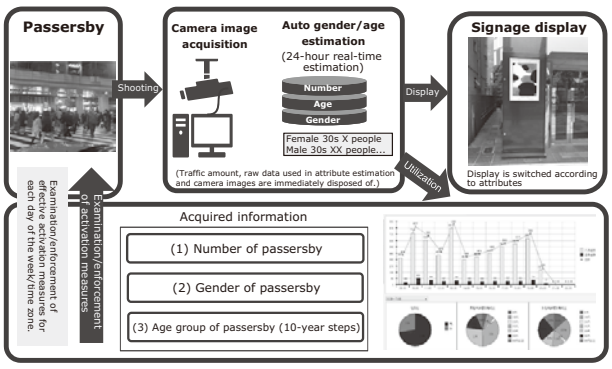

Fig. 2 Outline of a demonstration experiment.

gestions that may induce accidents/crimes and present a congestion-preventing guidance plan in real time, NEC conducted a demonstration experiment of a technology for real-time, accurate estimation/prediction of the congestion degree and the flow of a large crowd of people. This was done by installing cameras on public roadways between a large stadium and the nearest station in 2016 (**Fig. 3**).

To prepare the demonstration experiment, NEC first posted notices explicitly specifying the purpose of the experiment and inquiry contact information near to the camera installation locations. However, even if detailed explanation is given on these notices, a passerby may have difficulty in understanding it. Therefore, NEC decided to explain the details via a webpage and by giving its URL and QR code on the notices. NEC also visited the relevant local government administrators, local assembly members and residents associations in order to give direct explanations in advance. Other additional measures taken included publication of the process of disposal of the data acquired from the cameras via a webpage.

Although this experiment resembled the case in section 3.1 in that it aimed at human flow analysis using cameras, it was able to obtain assent from many persons concerned, perhaps because of the applied privacy measures as described above.

4.3 Brief summary

The present section describes cases of human rights and privacy considerations, but it cannot be affirmed that these issues can be avoided by uniformly applying the measures introduced above. This is because the ways of thinking vary depending on age, country and region as mentioned before. What is most important for the company is to think sincerely about considering the human rights and privacy of citizens by taking a case-by-case approach to each project.

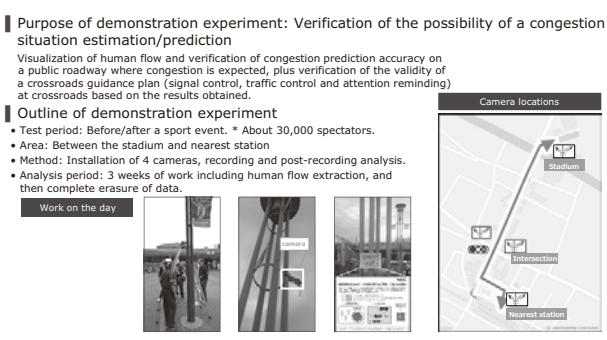

Fig. 3 Demonstration experiment for a large-scale event.

The efforts described in the present section can be regarded as the practice of the Privacy by Design (PbD)[6]. The PbD was proposed in the mid 1990's by Dr. Ann Cavoukian, who was a privacy commissioner in the state of Ontario, Canada. It is today the approach accepted as a world standard of privacy protection and it is referred to in the policy studies of many countries (**Fig. 4**).

Today, as discussed in section 3.2, the advancement of AI (Artificial Intelligence) and of the biometrics technology poses worldwide issues, which are not limited to privacy but also include bias/discrimination and mass surveillance by governments, particularly with the relationship of the applications of facial recognition systems.

To deal with such problems, NEC has installed the Digital Trust Business Strategy Division in order to expand the idea of PbD over the entire human rights sector based on Human Rights by Design (HRbD). This is a concept that incorporates the notion of respect for human rights, such as fairness and privacy into each process of the value chain. As part of this approach, NEC establishes a company-wide policy this April based on HRbD and proceeds to joint research with Keio University Global Research Institute, aiming at listing the checkpoints to be considered by business operators from the viewpoint

1. **Proactive not reactive; preventative not remedial**
2. **Privacy as the default setting**
3. **Privacy embedded into design**
4. **Full Functionality - Positive sum, not zero sum**
5. **End-to-end security - Full lifecycle protection**
6. **Visibility and transparency - Keep it open**
7. **Respect for user privacy - Keep it user-centric**

Fig. 4 Seven fundamental principles of privacy by design.

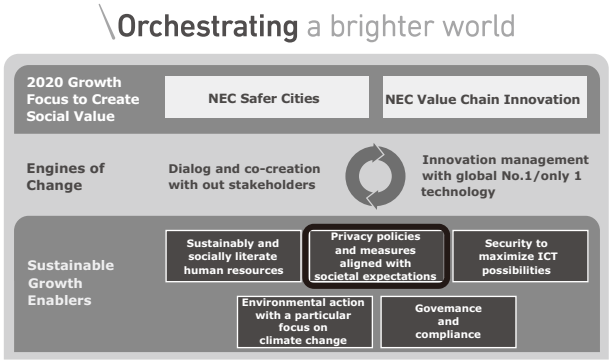

Fig. 5 "Materiality", the priority management themes from an ESG perspective.

of HRbD. NEC also identified "privacy policies and measures aligned with social expectations", which is one of the "Materiality", priority management themes from an environmental, social, and governance (ESG) perspectives. It also declared that it would make whole-group scale efforts towards this end (**Fig. 5**).

5. Conclusion

In the above, the paper discusses the human rights and privacy measures of biometric businesses by particularly focusing on cases in which cameras are used.

The advancement of AI and biometric technologies is expected to make the idea of respect for human rights such as privacy and fairness more important than ever in the future[7].

By applying its acquired knowledge as a leading technology company NEC will address these issues head-on to help create a better society and sustainable growth of the company.

* QR code is a registered trademark of DENSO WAVE INCORPORATED.
* All other company names and product names that appear in this paper are trademarks or registered trademarks of their respective companies.

Reference

1) Mitsubishi Research Institute, Inc.: *Kojinshikibetsu fugou ni kansuru kaigai kokunai dōkō no chosa kenkyu hokokusho*, 2018.3 (in Japanese) https://www.ppc.go.jp/files/pdf/201803_kojinshikibetsu_fugou.pdf
2) e.g. FEDERAL TRADE COMMISSION: Facing Facts: Best Practices For Common Uses of Facial Recognition Technologies, 2012.10 https://www.ftc.gov/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies
3) Toshiyoshi Miyazawa: *Kenpō / II Kihontekijinken shinpan*, Yuhikaku, 1971 (in Japanese)
4) *Eizo Censor Shiyou Daikibo Jissho Jikken Kentou Iinkai: Chosa Hokokusho (Survey Report by the Study Committee for Large-Scale Demonstration Experiment Using Image Sensors)*, 2014.10 (in Japanese) https://www.nict.go.jp/nrh/iinkai/report.pdf
5) NEC Press Release: *Roppongi Shotengai ni oite machizukuri no sesaku kentou no tameno ICT o katsuyou shita jissho zikken o kaishi*, 2017.10 (in Japanese) https://jpn.nec.com/press/201710/20171020_01.html
6) Ann CAVOUKIAN, Masao HORIBE (Ed), et al: Privacy by Design, Nikkei Business Publications, Inc., 2012.10
7) Tatsuhiko YAMAMOTO (Ed): Artificial Intelligence and the Constitution of Japan, Nikkei Publishing Inc., 2018.8

Authors' Profiles

SAMESHIMA Shigeru
Assistant Manager
Digital Trust Business Strategy Division

Information about the NEC Technical Journal

Thank you for reading the paper.
If you are interested in the NEC Technical Journal, you can also read other papers on our website.

Link to NEC Technical Journal website

Japanese English

Vol.13 No.2 Social Value Creation Using Biometrics

Vol.13 No.2
April 2019

Special Issue TOP

Papers for Special Issue

NEC Information