




Governance Framework for Facial Recognition Systems in Japan

Aimi Ozaki^(✉) 

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

Abstract. With the evolution of machine learning, the facial recognition technology has already been used in different kinds of situations. In a field where such technological developments have a significant impact on society and the people who live in it, rulemaking is carried out by a variety of actors. Therefore, the METI suggests that what is most important is how quickly rules can be changed in line with technological innovations and the changes in business settings resulting from such innovations and how we can build a mechanism for such changes. This paper introduces how the Japanese government and the private sector analyze the risks posed by using the face recognition technology. Then, the issues of these analyses are discussed. Generally, businesses are at the heart of using personal data to drive innovation and create value for society. As a result, they are expected to play a central role in the design of governance. Also, given the nature of face recognition, which fosters discrimination and surveillance, this paper introduces some ideas that can be used as a reference point for businesses to consider when establishing governance in the use of the face recognition technology.

Keywords: Facial recognition · Privacy · Personal data · Algorithmic bias · Fairness

1 Governance Design in the Facial Recognition Technology

1.1 The Development of the Facial Recognition Technology

With the evolution of machine learning technologies and algorithms, the facial recognition technology has been used in many kinds of situations [1]. The facial recognition technology is a type of biometric authentication technology that can automatically identify a person based on his or her physical and behavioral characteristics. The biometric technology is a technology for identification, and it is classified into two types: those that use physical characteristics and those that use behavioral characteristics. The facial recognition technology is categorized as the former type [2]. In general, face recognition is defined as an authentication method in which a person is identified by comparing his or her face information, which is captured using a camera, with other face information in a database. There are two types of face recognition: “active authentication,” where the person is authenticated with his or her consent, and “non-active authentication,” where the person is authenticated without being aware of

it. An example of the former is the identity verification system, which is used at events to determine if a person who purchased a ticket is the same one who enters the venue. An example of using the face recognition technology for investigative purposes is to search for wanted criminals and suspects on the run. In such cases, it would be difficult or almost impossible to obtain the consent of the wanted criminals or suspects for using face recognition. Therefore, the use of the face recognition technology for investigative purposes is considered a “non-proactive authentication [3].”

1.2 The Need for Governance Design in the Facial Recognition Technology

In a field where such technological developments have a significant impact on society and the people who live in it, rulemaking is carried out by a variety of actors. The rules of each country influence each other and are increasingly cross-referenced in many situations. Furthermore, international harmonization is increasingly necessary for such situations. The actors in this context include the state, citizens, companies, and platforms. Therefore, the METI (Ministry of Economy, Trade and Industry) suggests that what is most important is how quickly rules can be changed in line with technological innovations and the changes in business settings resulting from such innovations and how we can build a mechanism for such changes [4, 5].

1.3 Direction of the Governance Design

The METI states that innovative technologies and services can also rapidly change the risk landscape. In this case, the risks include the following. In data collection and management, digital service providers collect enormous amounts of accurate personal data, such as a person’s behavior history, health status, economic activities, thoughts, beliefs, hobbies, and preferences, thus raising many privacy risks. For example, the use of such personal data in targeted political advertisements can potentially cause harm to democratic systems. In areas of data analysis, since the autonomous decision-making by algorithms, which involves no human intervention, now takes over important positions in society, the necessity to discuss the safety and adequacy of such algorithms is increasing. Since machine learning is not based on static rules and its outputs are dynamically produced by adjusting the weights of variables through statistical processes, it is difficult to fully predict its behavior. Additionally, in the case of deep learning algorithms, even if a decision made by a specific algorithm is found to be inadequate, we are currently faced with the problem that the cause of such behavior can sometimes be difficult to explain. When these outputs of the algorithms are fed back into the physical world, there are risks of unpredictable accidents, magnifying discriminations, and unfair bias driven from datasets [6].

Unlike the DNA, which contains genetic information related to diseases, etc., face information does not have a high degree of privacy on its own. However, the facial recognition technology integrates (links) the face information with other personal information, which transforms the nature of the face information into a high degree of privacy. In the use of the facial recognition technology, an individual’s face information can be collected by businesses and other entities. Businesses are at the heart of

using personal data for driving innovations and creating social values. As a result, they are expected to play a central role in the design of governance. Thus, it is necessary for society to properly control the risks posed by such innovations and to design governance that realizes various social values, such as privacy, democracy, and anti-discrimination.

Governments are also supposed to make flexible and appropriate decisions depending on the risks posed by different innovations and the situation concerning the corporate self-regulations and guidelines of various organizations. In addition, they need to be equipped with the necessary expertise so that they can be able to make decisions on whether regulations would be necessary or not.

Accordingly, in the next chapter, this paper introduces how the Japanese government and the private sector analyze the risks posed by the use of the face recognition technology. Then, the issues of these analyses are discussed.

2 Guidelines Provided by the Government and Organizations in Japan

2.1 Report for the Large Face Recognition Study in the Osaka Station

The NICT (National Institute of Information and Communications Technology) planned to begin a large-scale face recognition experiment in April 2014 with the aim of improving the emergency response in the events of disasters. The NICT planned to install 92 digital video cameras in the Osaka station to film passers-by and test whether or not it is possible to create human traffic information. The purpose of this experiment was to perform a human flow analysis based on the face information acquired from the surveillance cameras and the face recognition technology. Also, the NICT spokesman emphasized that the data cannot be used to identify people and that it will abide by Japan's Personal Information Protection Law when it is handled. However, the experiment was met with so much criticism that it was eventually postponed.

A report on this experiment was submitted by an independent committee, which made the following observations. "In today's society, where the advanced digital technology and the Internet are widely used, extracting the individual's unique information from images of the whole body and face, etc. makes it possible to collect and record behavioral history without consent. This has the potential risk of harming the privacies of life. Consequently, the interest in not having such information extracted without due diligence constitutes a right to privacy. Then, the interest deserves legal protection. In addition, the average facial data required to generate feature information from facial images may be publicly available. Algorithms for extracting the feature information may be made available to the public as well. If so, third parties can use these to track individuals and obtain their behavioral histories. Moreover, the feature information generated from facial images and gait patterns cannot be changed unlike passwords. They require the same level of legal protection as biometric information such as fingerprints, iris and DNA information. Even if the risk of re-identification of a particular individual is minimized by the implementation of thorough security measures, it is assumed that there are those who wish to refuse to be photographed. The

location for video cameras is a place where people using the Osaka Station have no choice but to pass through. Therefore, some means of refusing to be photographed should be provided.”

2.2 Opinion Concerning the Legal Restrictions on Facial Recognition Systems

The Japan Federation of Bar Associations (“JFBA”) prepared its “Opinion Concerning the Legal Restrictions on Facial Recognition Systems” on September 2016 [7]. 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, and conduct searches in a pre-generated database of facial recognition data of specific people, 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.

2.3 Guidebook on the Processing of Personal Data in One ID Service in Airports Utilizing Face Recognition Technology

In March 2020, the Civil Aviation Bureau of the Ministry of Land, Infrastructure, Transport and Tourism (MLIT) established Guidebook on the Processing of Personal Data in One ID Service in Airports utilizing Face Recognition Technology. The One ID service uses the facial recognition technology to verify the identities of passengers during international flight departure procedures. The Narita and Haneda airports introduced the One ID service with the aim of making the boarding process faster. This is the first official guideline that specifically addresses the handling of the face recognition technology in Japan, and it serves as a basis for the formation of a norm for the future use of biometric information. Also, many businesses use this guideline as a reference.

Face information is a highly immutable identifier that can easily be obtained without a user's intention. In addition, there have been some cases in which people have strongly objected to the use of face recognition for tracking purposes. Therefore, in the use of the face recognition technology, not only do organizations have to comply with the Personal Information Protection Law and other relevant laws and regulations, but they also have to make sure that it is necessary to provide passengers with a clear explanation of the purpose of use and of the information management procedures. The guideline focuses on the following three points as ways to deal with privacy risks.

(1) Limitation of the purpose of use

The use of personal data should be limited to the boarding process only. Even if new needs arise in the future, the purpose of use should not be easily expanded or changed. In addition, the terms and conditions for handling personal data to be used should be clearly displayed to passengers.

(2) Secure traditional procedures

Only the passengers who wish to use procedures that utilize facial recognition should be allowed to use it, and some procedures that do not need facial recognition should remain in place.

(3) Retention period of the personal data

The used personal data in the One ID service should be deleted when the purpose of use is achieved and is no longer needed. The specific procedure is to delete the data within 24 h, and periodic audits of the service should be conducted.

2.4 Brief Summary

The risks in these guidelines concentrate on privacy. However, in recent years, other countries have pointed out that facial recognition has the potential to promote mass surveillance and discrimination. As mentioned in the introduction, the METI states that outputs of the algorithms are fed back into the physical world, there are risks of unpredictable accidents, magnifying discriminations, and unfair bias driven from datasets. In fact, privacy is not the only issue in the recent flaming cases in Japan. In the next chapter, this paper focuses on some recent cases and the new issues that are now discussed.

3 Recent Flaming Cases in Japan

3.1 Project Against Bookstore Shoplifting in Shibuya

In July 2019, bookstores in Shibuya started a joint project to share the facial image data of shoplifters and other relevant data with each other, and they used facial recognition cameras to detect the entry of shoplifters into their stores. Regarding the detection procedure, for example, a bookstore uses a facial recognition system to detect a subject's visit with a security camera. Then, the system notifies the clerk via a smartphone notification that a subject has entered the store. Afterward, the clerk calls out to the subject. Since it is not clear whether the subjects intend to shoplift or not, the clerks usually consider them to be criminals.

In order to ensure the protection of personal information and privacy, the project required compliance with the following requirements.

1. Compliance with the Personal Information Protection Law, etc.
2. Prohibition of use for purposes other than the intended use and the maintenance of confidentiality
3. Ensuring the information accuracy
4. Appropriate operation of the system for utilizing security images
5. Maintaining awareness as a member of the participating shops
6. Study of the operation personnel

3.2 JapanTaxi Use of Facial Recognition for Creating Targeted Ads

The JapanTaxi company installed tablets in the backseats of its vehicles, where the tablets have facial recognition systems for scanning the faces of passengers so as to determine their gender, age, and other characteristics. The purpose of the system is to deliver targeted ads to the on-board tablets. The existence and purpose of the cameras

were announced on the JapanTaxi website, and the facial recognition tablet has been in use.

After the service was launched, a Google engineer, Rosa Golijan, posted a photo of the warning on this tablet, which says “This taxi tablet is using a face recognition system with an image received by the tablet’s front camera. The image data is used to estimate gender in order to deliver the most optimized content. The gender estimation runs once at the beginning of the advertisement program and the image data is discarded immediately after the estimation processing. Neither the tablet nor the server records the data.” Her tweet was attached to a face with one eyebrow-raised emoji. The tweet led to a flurry of criticisms of JapanTaxi, and the issues at stake were privacy and gender, where the following criticisms were raised: “There is a problem with changing ads based on gender. It is based on the prejudice that women will like this stuff,’ but there is no basis for that prejudice. For some people, gender and sexuality do not match. It encourages a biased view of gender.”

In September 2019, The Personal Information Protection Commission (PPC) issued an administrative directive to JapanTaxi, and it was the second directive. As a result, JapanTaxi has revised its privacy policy, and it is now in the process of informing its passengers of the acquisition purpose in the clearest manner possible.

3.3 The Demonstration Experiment of the Osaka Metro Ticket Gate with the Facial Recognition System

In December 2019, the Osaka Metro began a demonstration experiment of a face recognition ticket gate. The target of the experiment was the employees of the Osaka Metro, and the period of the experiment is from December 2019 to September 2020. This face recognition system takes a picture of a user’s face with a camera when he or she passes through the ticket gate. Then, the acquired face feature data is sent to the server. This data is checked against a pre-registered face photograph. If the data is verified, the door of the ticket gate is opened. The facial recognition camera is constantly running, but it is not recording. As soon as it detects a subject’s face, the system converts the face into feature point data, which is then used for verification against the authentication server. The acquired images are managed on a dedicated network that is not connected to the outside world, and the acquired images are not used for any purposes other than the verification. The period of use of the recorded data shall be less than six months after the data is acquired. The expired data is either destroyed or processed in a manner that prevents the identification of individuals, and the verification data may be provided to cooperating manufacturers; however, the use of the data for other purposes is prohibited.

A spokesman for the Osaka Metro said that it would cooperate with the police if asked to provide information for investigative purposes. The Osaka Metro has also indicated that it intends to extract and use attribute data, such as gender and age data, from the personal information. According to some reports, although face matching with sunglasses and masks is not possible, it is possible to perform face matching with a photograph of the subject’s face.

4 Summary of the Issues

The criticism found in the flaming cases can be summarized from three perspectives.

4.1 “Database-Related Issues”

First, there are concerns regarding the expansion of the range of the collected face information in the database and the retention period of this information. This is a concern about the database itself, which is the collection and storage of information. In this paper, this issue will be referred to as the “Database-related issues.”

In the initial sense, each face is exposed to the public, and the face itself is not confidential. As mentioned at the outset, the face information, unlike the DNA, which contains genetic information related to diseases, etc., does not have a high degree of privacy on its own. Face images can be acquired without the invasion of the human body. Thus, the impact of the face information acquisition is smaller than that of forced urine or forced blood collections. According to a Japanese precedent, any person has the right not to have his/her face or appearance photographed without consent or good reason, and if a police officer, without good reason, has photographed a citizen’s face or appearance, such an act is in violation of the purport of Article 13 of the Constitution and therefore it is unallowable [8]. This precedent has not yet lost its force. Nonetheless, in the present-day society, facial images can be collected through open-source social media without the subject’s consent. Also, the facial recognition technology integrates (links) the face information with other personal information, which transforms the nature of face information into a high degree of privacy.

4.2 Concerns Regarding the “Surveillance Society”

The Osaka Metro has stated that it may provide the collected face information to investigative agencies. In this case, the facial recognition system could act as a surveillance device for investigative agencies.

As such, facial recognition can be used for mass surveillance. The fundamental rights considerations in the context of law enforcement according to the European Union Agency for Fundamental Rights (FRA) states that the use of facial recognition technologies can have a negative impact on the freedom of assembly if people fear that the facial recognition technology is used to identify them (“chilling effect”) [9]. The City of San Francisco has banned the use of face recognition technologies by San Francisco government agencies because “the propensity for facial recognition technology to endanger civil rights and civil liberties substantially outweighs its purported benefits, and the technology can exacerbate racial injustice and threaten our ability to live free of continuous government monitoring [10].” Consequently, it is necessary to prevent the use of the face recognition technology for promoting the “surveillance society.”

4.3 Does Facial Recognition Create Discrimination?

The case of the JapanTaxi is an example that gender discrimination may occur depending on the use of the facial recognition technology. Even in other countries, it is argued that the facial recognition technology is racial. The GDPR provides that processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited. In February of 2018, MIT researcher Joy Buolamwini and Timnit Gebru, then a Microsoft researcher, published a study that facial recognition systems have a harder time identifying women and darker-skinned people [11].

5 Conclusion

5.1 Towards Solving “Database-Related Issues”

Modern information technology has made the boundaries between short-term and temporary storage and the creation of databases extremely blurred. Thus, “the collection of information on the basis of short-term preservation should be clearly grounded and controlled by law [12].” According to this view, on the contrary, with the law and the oversight agencies created by the law to make sure that the information is not stored in the long term, many of the privacy issues can be eliminated. In turn, what powers should be granted to such an oversight body? In light of the present situation where the collected face information by the private sector is used by government agencies without a warrant, it is necessary for an independent agency to oversee a series of steps for biometric information, including face information, so as to support the responsible use of the face information, conduct audits, and apply sanctions [13]. In Japan, the Personal Information Protection Commission (PPC) can be the equivalent of this agency. If it were so, the establishment of a commissioner specializing in biometric information as part of the PPC should be proposed.

5.2 How to Avoid Becoming a “Surveillance Society”?

Digital service providers collect precise and vast amounts of personal data, which enables them to precisely understand an individual's behavioral history, health status, economic activities, thoughts, beliefs, hobbies, and interests, etc. Facial recognition can create a “data stigma.” Therefore, businesses that provide such services should not reveal any special care-required personal information. Meanwhile, personal controllability should be ensured for customers.

5.3 Anti-discrimination

Before introducing the facial recognition technology, it is necessary for businesses to consider whether fairness is assured for the face recognition technology. Concretely, businesses (especially engineers) need to make sure that development shall not cause

discrimination. Also, businesses should be aware that such discrimination can easily occur [14].

Recently, in response to the growing anti-discrimination movement, a number of companies have stopped providing facial recognition systems to criminal investigations. For example, on June 8, 2020, IBM said that it would stop offering facial recognition software for “mass surveillance or racial profiling” to respond to the death in police custody of George Floyd. Amazon has also banned the police from using its controversial facial recognition software for a year.

However, the facial recognition technology should not be uniformly banned. Rather, it is easier to detect fraud in algorithms than in humans, and it is easier to correct fraud in algorithms than in humans. By choosing the appropriate criteria, it is possible to construct algorithms that comply with fairness. It is also possible to increase fairness by using the facial recognition technology appropriately. It is necessary to carefully collect input and test data, generate models, and perform appropriate audits when using the facial recognition technology. It is also important to categorize the purposes and targets of using face recognition technology in detail [15]. There is a need for businesses to put in place an appropriate audit system for the use of technology to avoid leading to those actions. Such a system would also give an advantage in gaining the trust of consumers.

5.4 Appendix: Principles for Proper Use of the Face Recognition Technology

As mentioned in the introduction, businesses are at the heart of using personal data to drive innovation and create value for society. As a result, they are expected to play a central role in the design of governance. Finally, given the nature of face recognition, which fosters discrimination and surveillance, this paper introduces some ideas that can be used as a reference point for businesses to consider when establishing governance in the use of the face recognition technology [16].

(1) Principle of the Self-Determination of Information

Businesses shall enable users to exercise their rights to the self-determination of information. Businesses should aim to design and implement user interfaces for this purpose.

(2) Principle of Effective Remedies

Businesses should understand the potential of harm to users and provide effective remedies for them.

(3) Principle of Providing Alternatives

Businesses should provide a way for users who do not agree with facial recognition to receive the same services as before.

(4) Principle of the Limitation of the Purpose of Use

Businesses shall use the user’s face information only for the purpose of its pre-determined use.

(5) Principle of Safety Management

Businesses must take security measures, such as encryption, non-retention, and information security audits, by third parties.

(6) Principle of Appropriate Use

Businesses should make sure that the facial recognition technology is not used in a discriminatory way.

(7) Principle of Transparency

Businesses shall establish a policy on how to respond to requests for the disclosure of information about users from law enforcement agencies.

(8) Principle of Non-Use of Excluded Data

Businesses shall not use data that is not included in the scope of the intended use.

(9) Principle of Preliminary Consideration

Businesses should consider each point of these principles in advance.

(10) Principle for Strengthening Communication

Businesses should ensure appropriateness throughout the supply chain, and they shall provide information relevant to the risks that may arise to users to strengthen communication.

References

1. <https://www.nec.com/en/global/solutions/biometrics/face/index.html>
2. Research and Legislative Reference Bureau National Diet Library, Current Trends in Biometrics, Research Materials 2018-6 http://dl.ndl.go.jp/view/download/digidepo_11257103_po_20180602.pdf?contentNo=1
3. Suzuki, T.: The biometrics with focus on video face recognition technology. *J. Inf. Process. Manage.* **60–8**, 564–573 (2017). https://www.jstage.jst.go.jp/article/johokanri/60/8/60_564/_pdf
4. Terada, M.: Public Law on Advanced Technology and Regulation, Keiso Shobo (2020)
5. Hioki, T.: Utilization of “face” information and act on the protection of personal information. *Bus. Houmu* **17–4**, P87 (2017)
6. The METI (Ministry of Economy, Trade and Industry), Governance Innovation: Redesigning Law and Architecture for Society 5.0 <https://www.meti.go.jp/press/2020/07/20200713001/20200713001-2.pdf>
7. Japan Federation of Bar Associations, Opinion Concerning the Legal Restrictions on Facial Recognition Systems <https://www.nichibenren.or.jp/en/document/opinionpapers/20160915.html>
8. Saikō Saibansho [Supreme Court] Dec. 24, 1969, Showa 44, Saikō Saibansho Keiji Hanreishu [Keishu] **23**(12), at 162 (1969) https://www.courts.go.jp/app/hanrei_en/detail?id=34
9. European Union Agency for Fundamental Rights (FRA), Facial recognition technology: fundamental rights considerations in the context of law enforcement https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf
10. Stop Secret Surveillance Ordinance <https://sfgov.legistar.com/View.ashx?M=F&ID=7206781&GUID=38D37061-4D87-4A94-9AB3-CB113656159A>

11. Raji, I., Buolamwini, J.: Actionable auditing: investigating the impact of publicly naming biased performance results of commercial ai products. In: Proceedings of the 2019 AAAI/ACM Conference on AI, Ethics, and Society, pp. 429–435 (2019) https://dam-prod-media.mit.edu/x/2019/01/24/AIES-19_paper_223.pdf
12. Yamamoto, T.: Consider the Right to Privacy Shinzansha (2017)
13. Mann, M., Smith, M.: Automated facial recognition technology: Recent developments and approaches to oversight. UNSWLJ. **40**, p. 121 (2017)
14. Zuiderveen Borgesius, F.: Discrimination, artificial intelligence, and algorithmic decision-making (2018). <https://rm.coe.int/discrimination-artificial-intelligence-and-algorithmic-decision-making/1680925d73>
15. Kamishima, T., Akaho, S., Asoh, H., Sakuma, J.: The independence of fairness-aware classifiers. In: 2013 IEEE 13th International Conference on Data Mining Workshops, pp. 849–858. IEEE (2013) <http://www.kamishima.net/archive/2013-ws-icdm-print.pdf>
16. NEC Corporation, Biometric identification (facial features) data between businesses empirical study on architecture for collaboration https://www8.cao.go.jp/cstp/stmain/b-2-13_200318.pdf
17. Hamann, K., Smith, R.: Facial recognition technology: where will it take us. American Bar Association Available at: https://www.americanbar.org/groups/criminal_justice/publications/criminal-justice-magazine/2019/spring/facial-recognition-technology/. Accessed 6 May 2019