WORLD
ECONOMIC
FORUM

COMMITTED TO
IMPROVING THE STATE
OF THE WORLD

White Paper

A Framework for Responsible Limits on Facial Recognition

Use Case: Flow Management

Pilot project

February 2020

World Economic Forum
91-93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland
Tel.: +41 (0)22 869 1212
Fax: +41 (0)22 786 2744
Email: contact@weforum.org
www.weforum.org

Contents

Introduction

Over the past decade, facial recognition has emerged as one of the most powerful biometric technologies, capable of identifying and verifying a person by comparing and analysing patterns based on that individual's facial contours. Improvements in facial recognition systems – due mainly to progress in machine learning and sensors – are expected to boost the market for this technology to $7 billion in 2024, compared to $3.2 billion in 2019.[1] Indeed, while the most efficient facial recognition systems achieved a respectable accuracy score of 72% in 2010, they now easily exceed 95%.[2]

Facial recognition technology has many applications, from improving consumer experiences in the banking and retail sectors to speeding up border control at airports. While the development of this technology creates considerable opportunities for socially beneficial uses, it also poses a serious threat to human rights and civil liberties – notably, freedom of expression, freedom of assembly and association, and the right to privacy. The overarching concern is that technologies which "collect and store information just in case it is needed are being transformed into technologies that actively watch people, often in real time",[3] as stressed by the American Civil Liberties Union (ACLU).

In recent years, public concerns about facial recognition technology have grown, fuelled by various controversies. Some retailers have used this technology without notice or consent,[4] an increasing number of schools are deploying it to monitor students,[5] data breaches of biometrics are regularly being reported,[6] and personal data is being used to develop facial recognition systems without asking users for permission.[7]

Although the progress in facial recognition technology has been considerable over the past few years, ethical concerns have surfaced regarding its limitations. Studies have shown[8] that facial recognition can be unfairly biased, performing differently based on demographic characteristics. A recent study found that both system accuracy and performance are affected by skin tone, which could lead to misidentification of individuals. Furthermore, gender, age, height, eyewear or a headscarf can also affect accuracy and performance, depending on the system. When used in real-time law enforcement scenarios, this could increase the risk of misidentification and potentially lead to significant safety concerns. In this context, we cannot be satisfied with the status quo. We must develop a governance framework to ensure the responsible use of facial recognition technology. We argue that this framework should be evidence-based and co-designed through a multistakeholder approach.

To this end, the World Economic Forum is spearheading a multistakeholder, evidence-based policy project in France focused on one use case scenario. The goal of this initiative is to establish a governance framework for facial recognition technology that has been tested on site. The main challenge here is to run various policy pilots around other use cases in France or abroad (taking into account local regulations, social norms and other contextual considerations) in order to continuously strengthen this framework for action.

Further, this framework aims to inform the public debate on the use of facial recognition technologies at the national, European and international levels. As this is an issue that concerns questions related to individual and collective rights and freedoms, citizens and their democratic representatives are the only legitimate decision-makers with respect to the uses they wish to promote or restrict and the conditions under which the technology should be used. Our ambition is to empower citizens and representatives as they navigate the different trade-offs they will face along the way. This white paper is the first step in an iterative process, And we welcome organizations willing to take part in this debate to join our project.

A policy framework to ensure the responsible use of facial recognition

1. Methodology

In order to design a balanced and actionable framework to ensure the responsible use of facial recognition, the Artificial Intelligence team of the Centre for the Fourth Industrial Revolution of the World Economic Forum has conducted a multistakeholder consultation and developed a method structured around four main steps:

- **Define** what constitutes the responsible use of facial recognition through the drafting of a set of principles for action. The first objective of the working group, composed of public figures, companies that design and procure facial recognition systems, regulatory bodies, academics and representatives of civil society, was to establish a shared definition, organized around 11 principles

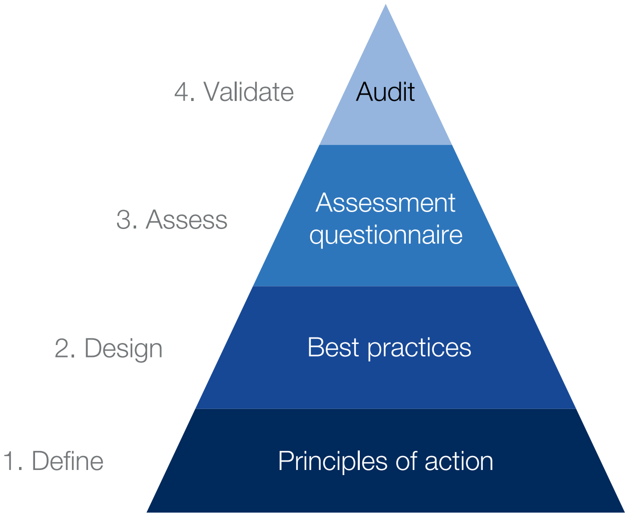
- **Design** a set of methodologies, tailored by use cases, to support product teams in the development of systems "responsible by design"

- **Assess** to what extent the system designed is responsible through an assessment questionnaire that describes for each use case what rules should be respected to comply with the principles for action

- **Validate** compliance with the principle for action through the design of an audit framework by a trusted third party

This method, which is intended to be deployed on a case-by-case basis, appears essential to us because the risks associated with the use of facial recognition technologies are highly context dependent.

The four steps to ensure the responsible design and use of facial recognition technology for flow management use cases



Working group

To achieve these objectives, a working group will collaborate on a French-based project to co-design an evidence-based policy framework, and to test and review it based on the outcomes of this framework for action.

Members of the working group have played two complementary roles:

- **Contributors:** industry representatives who are considering procuring facial recognition systems (Groupe ADP and SNCF), technology providers (Amazon Web Services, IDEMIA, IN Groupe and Microsoft), policy-makers (members of the French Parliament, OPECST), academics, civil society organizations and AFNOR Certification

- **Observers:** the French Data Protection Authority (Commission Nationale de l'informatique et des libertés [CNIL]) and the French Digital Council (Conseil National du Numérique)

Programme

The pilot project will take place over 18 months, according to the following schedule:

- Scoping (April to September 2019): identify potential applications of facial recognition technology and the relevant stakeholders

- Co-designing (October 2019 to January 2020): building a policy framework that includes a set of principles for action, a set of best practices, an assessment questionnaire and an audit framework:

  - **Principles for action** define what the responsible use of facial recognition technology could encompass.

  - **A set of best practices** provides designers and users of facial recognition technology with concrete guidelines on how to design a system “responsible by design”.

  - **The assessment questionnaire** operationalizes these principles for the selected use case, enabling organizations to assess their risk mitigation processes.

  - **The audit framework** ensures that organizations are effectively compliant with the principles for action. This work will be done by AFNOR Certification. As an initial matter, the audit framework should be based on a review of the assessment questionnaire. The conduct of the audit will ensure that the questionnaire meets the objectives of the governance framework. In this regard, we encourage external audits done by third parties. It may also be appropriate to consider the potential for self-audits, supplemented by audits done by independent organizations.

- Testing (February to July 2020): testing this policy framework on a specific use case and reviewing it (which includes the principles for action, set of best practices, assessment questionnaire and audit framework)

- Deploying (from July 2020): supporting the deployment of the policy framework through several scenarios (the choice of which will be made later in the project – it could be one or a combination of the following scenarios):

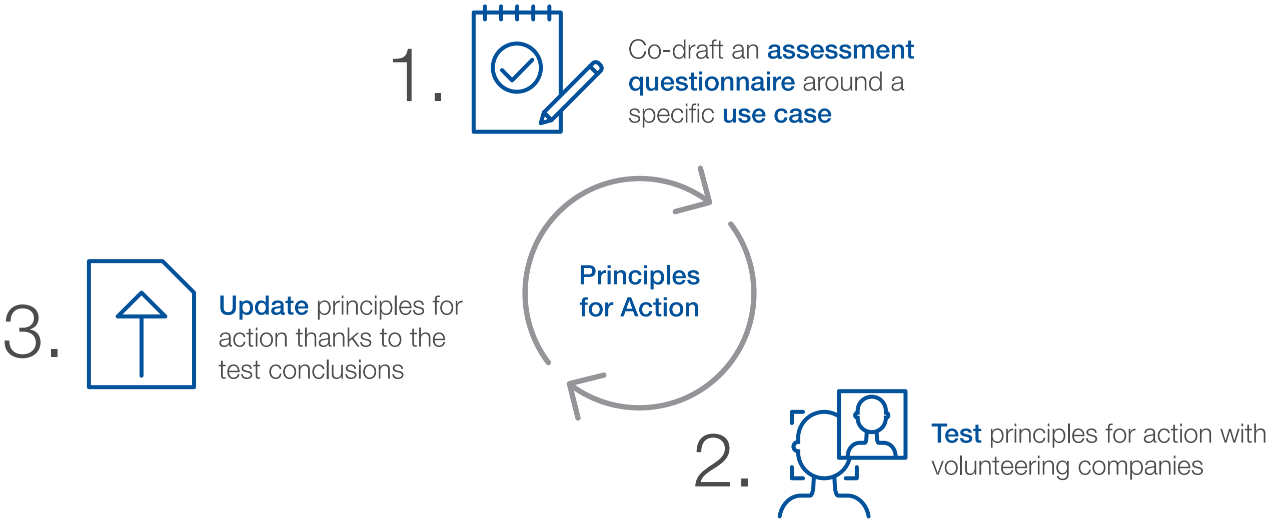
  - **Scenario 1:** The framework is endorsed by companies that design or procure facial recognition systems

  - **Scenario 2:** Support the deployment of a standard or certification process using this framework in order to create a sustainable accountability mechanism

  - **Scenario 3:** Support the adoption of a legislative framework to both enable similar policy pilots and ensure compliance with the Principles for Action

The pilot phase will follow this journey

Illustration of testing process for policy project use cases



1. Co-draft an **assessment questionnaire** around a specific **use case**

Principles for Action

2. **Test** principles for action with volunteering companies

3. **Update** principles for action thanks to the test conclusions

2. Identified use cases

Approaching facial recognition through different use cases enables a better understanding of the trade-offs that need to be addressed. The only purpose of this list is to illustrate the current and potential use cases with which we can test our policy framework, in accordance with relevant national laws.

Use cases
Face access

Use cases
Safety and security of public spaces

Use cases
Marketing and customer services

Use cases
Healthcare services

Face access

Use cases included in this category relate to end-user access to public or private services. This includes, but is not limited to:

- Flow management: replacing tickets with facial recognition to access physical premises or public transport, such as train or subway platforms, boarding aeroplanes and buses, access to stadia, concert halls, music festivals and public events with large audiences, and VIP access
- Face as a key: access to hotels, houses and apartments
- Unlocking a device: a smartphone, a computer or a vehicle
- Payments and financial operations: ATM access, cashier payment, cashier-less payment and automated payment
- Username and password alternative: log in for online services
- Onboarding online and offline services: age verification, ID verification, hotel check-in and airport check-in
- Legal authentication: access to public premises that should require an ID, identifying prison visitors, authentication as a citizen – access to voting polls and replacement of ID or passport

Safety and security of public spaces

This includes law enforcement and private security activities including but not limited to:

- Customs and border protection: identity control
- Person of interest tracking based on a warrant or terrorism risk
- Neighbourhood watch: private front-door cameras or external cameras on vehicles used for facial recognition
- Search for missing persons
- Private security: tracking shoplifters and burglary prevention
- Safety at public events, such as demonstrations and carnivals
- Safety in public spaces: automated CCTV, schools, subway or train stations and movement tracking
- Police patrol: body cameras
- People attendance: tracking student attendance

Marketing and customer services

This includes all marketing, advertising and customer services based on facial recognition including but not limited to:

- Personalized shopping: personalized beauty recommendations, advertising based on what customers are looking at or their position in the store and tracking customers in cashless stores
- Automated recognition of photos on social media
- Gamification of faces and entertainment: personalized emojis, filters, lenses to modify faces or run live augmented reality
- Emotion recognition: advertising and services based on emotions and facial expression, car safety (tracking attention of drivers), pre-hiring assessments

Healthcare services

This includes all medical-based and patient services using facial recognition:

- Consumer wearables for blind or partially sighted people: facial recognition to identify people
- Patient authentication: to avoid mistakes or confusion between patients
- Identify or track pathologies: improving autism diagnosis and screening, cardiovascular anomalies, diabetes identification, diagnostic of congenital and neurodevelopmental disorders

3. Principles for Action

3.1. How to use the Principles for Action

As stated, this first version of the Principles for Action will be reviewed based on the practical findings of the policy pilot. Any organization, public or private, that is interested in applying the principles to a similar pilot should ensure that its use case is lawful. We advise companies to abide by the following recommendations:

Be lawful: that is, acting in compliance with relevant national and regional legislations, and in the case of the EU, ensuring that the deployment of facial recognition respects the General Data Protection Regulation (GDPR). The company/organization using the technology should also produce a data protection impact assessment (DPIA), available upon request from competent data protection authorities. Accordingly, we strongly encourage organizations willing to run an evidence-based policy pilot on facial recognition technology to inform the relevant data protection authorities beforehand.

Be audited by a third party: to operationalize and test these principles, AFNOR Certification has developed an audit framework. The audit framework will help assess the effectiveness of the risk management and governance processes implemented by an organization willing to comply with the principles presented below. Although this audit can be performed internally, we encourage organizations to identify an independent third party able to conduct an external audit.

Report to an oversight body for the policy pilot: any organization interested in running an experiment on a specific application of facial recognition should get in touch with the appropriate regulatory body within its jurisdiction. In the EU, it would be the competent national data protection authority – for example, the CNIL in France. It is worth noting that the CNIL has recently published a position paper explaining how an experiment in facial recognition technology should be designed and conducted.[9]

Run an impact assessment on sensible use cases: this project is not an assessment of facial recognition technology, but rather a pilot to test a policy framework to ensure its responsible use. To this end, we encourage organizations willing to experiment with facial recognition – for example, in public spaces – to run an impact assessment. The trade-offs in some use cases can't be resolved without a public debate and an appropriate methodology to measure the feasibility of using facial recognition. In this regard, the National Institute for Research in Computer Science and Control (INRIA) has recently published a detailed methodology on how to run an impact assessment.[10]

3.2. First version of the Principles for Action

The first version of these principles has been co-drafted through a multistakeholder process, while paying careful attention to the EU GDPR[11] and the police and criminal justice directive,[12] and has drawn inspiration from some of their principles. We also considered the Ethics Guidelines of the High-Level Expert Group on Artificial Intelligence of the European Commission as a vital document that paves the way for an ethical use of AI technologies across the EU.

These principles are meant to ensure the responsible use of facial recognition technology. In this respect, they don't cover any other biometrics, including DNA, fingerprint, iris or gait recognition. Finally, these principles represent the first milestone in this policy project and should be reviewed with reference to the findings of the policy pilot on site. During the testing phase, we will pay particular attention to their potential for effective implementation, completeness and relevance.

Bias and discrimination

Organizations using facial recognition systems should take appropriate steps to ensure that unfair bias or outcomes can be detected, identified and mitigated to the greatest extent possible. While acknowledging that the complete removal of bias represents one of the biggest challenges in AI research, organizations must allocate appropriate resources to the implementation of tools and processes that minimize unfair bias or outcomes.

Proportional use of facial recognition systems

Organizations using facial recognition systems should take reasonable steps to assess the capabilities and limitations of the systems they intend to use and ensure that their systems are appropriate for purpose. Facial recognition systems should be highly tailored according to the intended use.

Privacy by design

Organizations using facial recognition systems should design systems to support privacy, including privacy considerations in system requirements and carrying through privacy support in the design, development and testing of technology as well as in supporting business practices and ongoing system maintenance.

Accountability

Organizations using facial recognition systems should ensure a culture of accountability internally and across third-party service providers or business partners. To this end, they should establish and publicly disclose the governance principles that guide the design and use of their systems.

This does not apply to the technical specifications of their systems in relation to the prevention of potential cyberattacks.

Risk assessment and audit

Organizations creating facial recognition platforms or using facial recognition as part of an experience or systems should conduct a comprehensive risk assessment of their systems, including the impact on privacy, potential for errors, susceptibility to unfair bias, vulnerability to hacking and cyberattacks, lack of transparency in the decision-making process and potential for civil rights infringements.

Performance

Organizations creating facial recognition platforms or using facial recognition as part of an experience or systems should follow the standards for evaluating the accuracy and performance of their systems at the design (lab tests) and deployment (field tests) stages. Performance assessments should be auditable by competent third-party organizations and their reports made available to users of the systems.

Right for information

Processes should be put in place to inform end users who have questions and/or need information on the use of facial recognition systems. End users should have access to their personal biometric data upon request.

Consent

Individuals should provide informed, explicit and affirmative consent for the use of facial recognition systems. Any time data subjects enrol for a new service powered by facial recognition technology, they should express clear consent with regards to the length of data retention.

Notice and consent

When used in public spaces, clear signage should be deployed to ensure an obvious communication with end users on the use of facial recognition. Areas where facial recognition systems are used should always be delimited and indicated to individuals. A visual sign should also inform individuals when the system is in operation.

Right to accessibility and children's rights

Facial recognition should not exclude anyone and should always be accessible to and usable by all groups of people, including elderly people and people with disabilities. It is recognized that there may be some instances, such as infants and children, in which an exception to this principle is appropriate and an alternative to facial identification should be offered.

Alternative option and human presence

A manual review (human overseeing) should be conducted for any use that could result in a consequential decision, such as causing a civil right infringement. In the case of a fully automated system, a fallback system with a human in the loop should always be in place in order to address exceptions and unexpected errors. An alternative option to the use of facial recognition should always be in place, and it should be a reasonable option.

Policy pilot on flow management

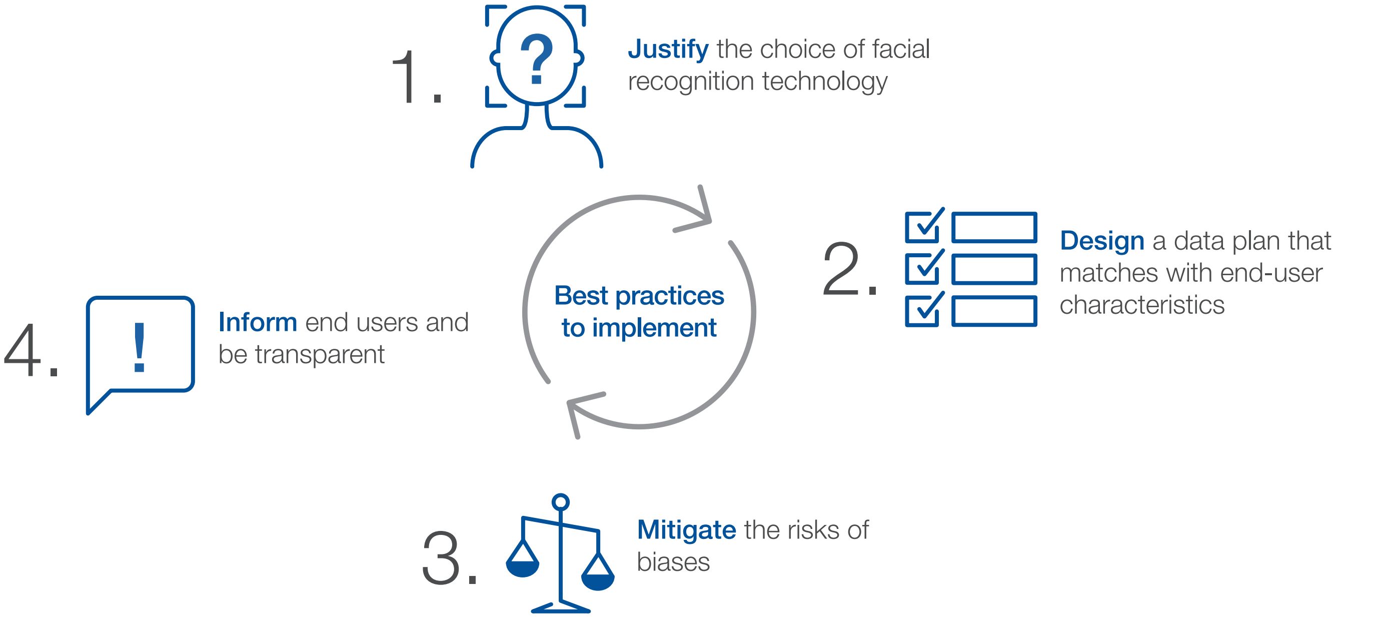
Among the various use cases presented above, the working group has decided to focus on "flow management" (face as a means to access a service) for the following reasons: first, this use case is likely to develop in the coming years. For instance, the organizers of the Tokyo Olympic Games have announced the use of facial recognition to manage the access of athletes and staff to stadia and Olympic facilities.[13] Also, airports and airline companies have started using this technology.[14]

Second, any facial recognition application has inherent risks. By recognizing this challenge and confronting the risks associated with its use for flow management, the project members have identified specific risks and thus designed insightful mitigation strategies.

Further, the method being applied here could serve as a blueprint for designers and users of facial recognition technology, which illustrates how to introduce ethical considerations into business operations.

1. Best practices to support the design of responsible facial recognition systems[15]

In order to facilitate the assessment of the responsible use of facial recognition technology for flow management use cases through the questionnaire presented below, designers and users of this technology should respect the following set of best practices for the design and deployment of facial recognition systems. These requirements focus on four main dimensions: (1) justify the choice of facial recognition technology; (2) design a data plan that matches with end-user characteristics; (3) mitigate the risks of biases; and (4) inform end users and be transparent. They should not only inform the work of product development teams but the entire organization's operations for both the providers and users of the technology. While they are relevant for various applications of facial recognition, they were purposely designed for flow management use cases. Also, they represent a *minimum* set of requirements that may be reviewed and completed based on the results of the policy pilot.



Best practices to implement

1. **Justify** the choice of facial recognition technology

2. **Design** a data plan that matches with end-user characteristics

3. **Mitigate** the risks of biases

4. **Inform** end users and be transparent

Justify the choice of using facial recognition technology

This implies defining the problem to be solved and explaining how facial recognition technology might better solve this specific problem compared with alternative technologies. Here, a review of the strengths and weaknesses that led to the decision to use facial recognition software would be highly valuable. In addition, organizations willing to deploy such technology should define what assumptions (e.g. likely false positive and false negative rates, likely performance outcomes, etc.) will need to be true to support the value of facial recognition for this purpose. If those assumptions have not been verified, they should collect data to validate them.

Design a data plan that matches with end users' characteristics

Based on the defined characteristics of the end users, a data plan needs to be designed that includes fairly equal samples of these subgroups and collects data accordingly. This data should also reflect conditions similar to those where the system will be deployed whenever possible. Even when using a pre-trained model, it is important to collect a test dataset, specific to the conditions of use and the characteristics of the end users, to evaluate the system for unfair biases. The data collected should be evaluated to ensure it aligns with the data plan.

Mitigate the risks of biases

Define the risks of unfair biases in the system to be developed for flow management use cases. To this end, organizations that provide or use facial recognition technology should:

- Evaluate each step in their process of use (for instance, unfair biases based on image capture and unfair bias based on model performance). Consider and document the impact of false positive and false negative errors in each case.

- Document the characteristics of the end users of your system, including age ranges, gender, countries of birth, race and ethnicity, and prioritize the groups for which you will evaluate bias and minimize differences.

  - Document the characteristics of people who need to be considered in the system design: How well will it work for people who are in wheelchairs or extremely tall? How will it work for people who wear turbans or other headwear?

  - For each of the risks of discrimination identified, determine how your organization evaluates the system for this bias: What metrics will be used? How will they be measured? What criteria must be met for each metric for the system to be considered ready for release?

- Define the environment in which each of the identified risks will be evaluated and how it reflects the environment of the deployed system.

Define and document how identified unfair biases will be mitigated

It is important to continually evaluate the risks and design mitigations throughout the development of the system. Some mitigations can be defined during the design phase, such as specifying sensor quality or building an environment for capture in which the lighting is well controlled. Other mitigations may already have been implemented by the provider of pre-trained algorithms, such as cropping photos to avoid including hair to improve accuracy for people who wear turbans or other headwear. Still others will require that the system design accommodates mitigation, such as providing good "fall-back" options, or allowing for quick retries to mitigate errors. No matter when a risk is identified or a mitigation is created, it is important to evaluate whether the mitigation is successful.

Evaluate the system to detect risks of unfair biases during the development process

The system should be evaluated for unfair biases several times during the development process to allow time for mitigation, as well as being assessed after it has been deployed but before being used as the production system. If any gaps remain that may result in harm to users, the system should not be released until the harm is mitigated or the gap is closed.

Build an implementation process

Processes should be implemented to define best practices and review systems for the detection, identification and mitigation of unfair biases.

Inform end users and be transparent.

End users should have easy access to:

- Relevant information about the functioning of facial recognition systems

- Governance principles that guide the design and use of the system into a format that is intelligible to non-experts

- A consent policy that includes a summary of important provisions (e.g. intended purposes, data retention periods, data protection and sharing policies)

The evidence must show that the capture space is understood by users and that the signage is noticeable and legible.

2. First version of the assessment questionnaire

The first version of the assessment questionnaire and principles for action was designed through a similar multistakeholder process. The main objective of this questionnaire is to enable a careful assessment of facial recognition systems deployed for flow management and to ensure their compliance with the Principles for Action presented in the first part of the white paper. Therefore, it is a tool meant to help organizations willing to operationalize these principles in the systems that they design or procure.

In this regard, the publication of the assessment questionnaire represents the second key milestone of our policy project, after the publication of the principles for action. Similarly, it is likely to evolve depending on the results of the pilot phase, which will be carried out soon. During the testing phase, we will pay particular attention to their potential for effective implementation, completeness and relevance. Finally, to help with reading the questionnaire, we have presented the assessment questions associated with each principle for action.

Bias and discrimination

- What are your definitions of unfair bias in your use case? Describe the metrics used to evaluate each of them.
- What is your risk analysis framework? Describe the risks of unfair bias identified for your use case and the groups described by end-user characteristics for which you evaluated bias.
- How are risks prioritized in this process? How are competing interests resolved?
- Please describe the existing best practices for detection, identification and mitigation of unfair biases that were applied in this case.
- What action plans have you put in place to mitigate the main risks identified? For each risk, what mitigation was identified and how were mitigations evaluated to ensure effectiveness?
- What are the test cases and acceptance tests used for your facial recognition system?
- What is the distribution of your training set and how well does it align with that of the end users of your system? If there are gaps, how did you evaluate the impact of the gaps and remediate them?
- What kind of trade-offs are you facing in the deployment of your system? How do you address them?
- If there are any gaps between the release criteria and actual performance, how are the gaps remedied?

Proportional use of the facial recognition system

- What are the alternatives to your facial recognition system? And why have you rejected them? What are the criteria used to determine the advantages and disadvantages of these alternatives?
- How did you assess the appropriateness of your system for its purpose?
- Describe the technical requirements for addressing the objectives of your system within a format understandable by the appropriate authorities.
- Have you carried out a risk analysis of the false positive and false negative situations (in particular, the risks of violating civil rights)?

Privacy by design

- What processes (e.g. a task force) and resources (e.g. a charter of best practices) have you implemented to support the privacy of end users? For example, in order to avoid the over-collection of biometric data in relation to the purposes of use.
- Have you established a data protection officer position?
- How do you train your facial recognition product teams to be “privacy by design” (including product managers, legal teams, UX designers, data scientists and developers) to ensure a high level of data protection?

Accountability

- What mechanisms have you introduced to ensure the transparent governance of your system (e.g. intended use and performance metrics)?
- Have you implemented a review and approval process?

Risk assessment and audit

- Have you rigorously assessed the risks related to the use of your system before (e.g. risk assessment framework) and during its operational functioning (e.g. audit framework) through the following dimensions?
  - Privacy
  - Errors
  - Unfair bias
  - Hacking and cyberattacks
  - Transparency in the decision-making process
  - Human and civil rights infringements

Performance

- For the lab and field tests, what existing standards (e.g. International Organization for Standardization [ISO], AFNOR Certification and European Committee for Standardization [CEN]) are you following to evaluate the accuracy and performance of your systems? What criteria were used to choose the standards and norms that you follow?

- Have you submitted your facial recognition system to the National Institute of Standards and Technology (NIST) for evaluation?

- What process have you established to ensure the auditability of the performance results of your facial recognition system? What steps have been taken to allow a sufficient audit by a third party?

- What is the relevance of the performance tests conducted concerning the use case that has been considered?

- How do you justify the chosen performance threshold that induces a theoretical rate of false positives and a measured rate of false negatives?

Right to information

- What processes have been implemented to keep end users informed about the use of your system and their biometric data? Also, what processes, including the means for escalation and remedy, have been implemented when the system is believed to have caused harm? Best practices include but are not limited to providing for customer support and enquiries:

  - Email address

  - Phone number

  - Customer support FAQ

  - Customer support chatbot

- Could an end user retrieve or ask to delete personal data (photo, video and biometric data linked to a person's identity such as account event history, consent history, biometric data deletion history, shared information, history of use of biometric data) in a machine-readable format within a reasonable period (e.g. no more than 30 days)?

- Have you established and publicly disclosed (e.g. on your website) the governance principles that guide the design and use of your system in a format that is intelligible to non-experts?

- Have you established any process that enables individuals to access relevant information about the functioning of the system anonymously?

Consent

Does the consent policy provide explicit and clear information to users and more specifically:

- Is the consent page accessible after, at most, two clicks and is it easily visible in the "profile" page?

- Is a summary of the main provisions available on this same page?

- Does this summary contain the following information:

  - A description of all intended purposes

  - The data retention period

  - The data-sharing policy (including with which third parties this data will be shared)

  - The means put in place to protect, secure and store data

- Is this summary concise, comprehensible to non-experts and less than the equivalent of two A4 pages in length?

- Does the page for giving or not giving consent allow users to do it for each of the existing purposes?

  - Are all of these options available on the same page?

  - Is the list of existing purposes up to date?

Notice and consent

- What means have been put in place to inform individuals that they are entering an area in which a facial recognition system is being used? Are these means visible and explicit enough for individuals? Is a user rights reminder display in place?

- For premises access, flow management and/or enrolment in a public space, does the volume of the recording zone not exceed the capture space defined and identified by the end users? How do you ensure that the capture space is understood by end users (please provide evidence based on evaluation/research/testing)?

- Does a display of sufficient size relay the purpose of the facial recognition system? How do you ensure that the display is noticeable and legible (please provide evidence based on evaluation/research/testing)?

Right to accessibility and children’s rights

- Can you detail how the system has been designed and evaluated to support elderly people and people with disabilities (including visual and auditory)?

- Is your facial recognition system accessible to everyone, including elderly people and people with disabilities?

- What resources have you allocated to support elderly people and people with disabilities?

- Mitigation for people with disabilities, children, families and others for whom the system does not work or is undesirable may be to use an alternative option that has been tested to determine that it works.

Alternative option/human presence

- Have you put in place a manual review process for situations in which the matching of a face and an identity document with a photo leads to a false negative, especially during the enrolment phase?

- For facial recognition systems, is the alternative option systematically implemented and:

  - Operated by human agents; are these operators trained to handle exceptional situations?

  - Reasonable; that is, it does not introduce disproportionately adverse consequences (e.g. doubling the time needed to go through the security check)

- Is there an alternative process for people who don’t accept the use of their biometrics?

Conclusion

Considering the sensitivity of biometric data, the use of facial recognition is intrinsically risky. This is true even when its use may provide recognized benefits to individuals and communities. Therefore, there is a pressing need for the creation of a robust governance framework to mitigate these risks. Designing such a framework requires drafting achievable principles, testing them on site and using the results of a policy pilot to review them. This process will ensure that the governance framework is reliable, protective and endorsed by various stakeholders.

To achieve this goal, we have built a multistakeholder community and applied a method structured around four main steps: (1) define principles for action; (2) design a set of best practices to support the application of these principles; (3) assess, thanks to an assessment questionnaire, if organizations are compliant with them; and (4) validate these principles through an independent audit. These four steps should not only help inform the design of responsible systems for flow management use cases but also ensure that their designers and users are effectively compliant with these achievable principles.

We strongly believe that to ensure the effective adoption of these Principles for Action, they must be embedded at the core of business operations and thus product teams should be able to put them into operation. Yet completing this journey requires strong cooperation between industry actors, policy-makers, academics and civil society representatives. If we manage to build a sustainable collaboration between these stakeholders, we will lay the foundations for the development of truly human-centred technology.

The next step of this project is to test our policy framework on site, assess its relevance and review it based on the observed results. This policy pilot will enable AFNOR Certification to test its associated audit framework and pave the way for the design of a standard for the responsible application of facial recognition. Once the pilot project is completed, we will build a multistakeholder coalition of actors committed to respecting and promoting this governance framework.

Considering our open and experimental approach, we encourage industry players, public actors, civil society representatives, policy-makers and academics to join us on this journey to strengthen our governance framework and ensure its impact.

Glossary

Accuracy of facial recognition: The accuracy of a facial recognition system is based on a combination of two conditions: (1) how often the system correctly identifies a person who is enrolled in the system; and (2) how often the system correctly finds no match for a person who is not enrolled. These two conditions, which are referred to as the "true" conditions, combine with two "false" conditions to describe all possible outcomes of a facial recognition system (see the definitions of true positive, true negative, false positive and false negative).

Algorithm: An algorithm is a series of instructions for performing a calculation or solving a problem, especially with a computer. Algorithms form the basis for everything a computer can do and are therefore a fundamental aspect of all AI systems. Among the most widely used algorithms for facial recognition, we can name DeepFace, created by Facebook in 2014, and FaceNet, created by Google in 2015.

Biometrics: Biometrics covers a variety of technologies in which unique identifiable attributes of people, including (but not limited to) a person's fingerprint, iris print, handprint, face template, voice print, gait or signature, are used for identification and authentication.

Computer vision: Computer vision is a field of computer science that works on enabling computers to see, identify and process images in a way similar to how humans do it, and then provide appropriate output.

Enrolment: Enrolment is the process of enrolling images of individuals for template creation so they can be recognized. When a person is enrolled in a verification system used for authentication, their template is also associated with a primary identifier that will be used to determine which template to compare with the probe template.

Explainability: Explainability is a property of AI systems that can provide a form of explanation for how conclusions are reached to improve decision understanding and improve trust from operators and users of the systems.

Face detection: Detection finds human faces and answers the question, "Are there one or more human faces in this image?"

Face identification (or one-to-many): This answers the question, "Can this unknown person be matched to an enrolled template?" Identification compares a probe template to all enrolment templates stored in a repository, so is also called "one-to-many" matching. Candidate matches are returned based on how closely the probe template matches each of the enrolled templates.

Face verification (or one-to-one): This addresses the question, "Are these two images the same person?" In security or access scenarios, verification relies on the existence of a primary identifier (such as a customer ID), and facial recognition is used as a second factor to verify the person's identity. Verification is also called "one-to-one" matching because the probe template (one person) is compared only to the template stored for the (one) person associated with the identification presented.

Facial recognition: Facial recognition is a biometric software application capable of uniquely identifying or verifying a person by comparing and analysing patterns based on the person's facial contours.

False negative: A false negative is a test result that incorrectly indicates that the person in the probe image is not enrolled and they are not matched when they have been enrolled. Depending on the use case of facial recognition, the consequences of false negatives can vary greatly.

False positive: A false positive is a test result that incorrectly indicates that the person in the probe photo is enrolled in the system when they have not been enrolled. Depending on the use case of facial recognition, the consequences of false positives can vary greatly.

Probe image: A probe image is an image submitted to a facial recognition system to be compared to enrolled individuals. Probe images are also converted to probe templates. As with enrolment templates, high-quality images result in high-quality templates.

Template: Images of people are converted into templates, which are then used for facial recognition. Machine-interpretable features are extracted from one or more images of an individual to create that individual's template.

True negative: In a true negative, the person in the probe image is not enrolled and they are not matched.

True positive: In a true positive, the person in the probe image is enrolled and they are correctly matched.

Contributors

We would like to thank our participating organizations and experts for their multiple contributions and active involvement:

Hicham Alaoui Fdili, Video Expert, SNCF

Didier Baichère, Member of the French Parliament

Charlotte Baylac, Public Policy Manager at Amazon Web Services (AWS), Amazon

Xavier Blondeau, Manager Video-protection, SNCF

Vincent Bouatou, Director, Innovation Lab, IDEMIA

Pascal Briand, Groupe ADP

Natasha Crampton, Head of Office of Responsible AI, Microsoft

Laurent Dahmani, Deputy Director, AFNOR Certification

Jean-Luc Dugelay, Professor of Image Engineering and Security, EURECOM

Louis-Thomas Fernandes, LAF expert, SNCF

Romain Galesne-Fontaine, Director of Institutional Relations and External Communication, IN Groupe

Hervé Genty, Head of Data Retail Safety, SNCF

Meeri Haataja, Chief Executive Officer and Co-founder, Saidot.AI

Bruce Hedin, Principal Scientist, H5

Gökçe Çobansoy Hizel, New Technologies Law Principal, Turkcell

Mihael Krauth, Engineer, OPECST

Jacquelyn M. Krones, Director of Responsible AI Practice, Microsoft

Jarrett Lane, Public Policy at AWS, Amazon

Gautier Martin, Project Manager, Groupe ADP

Franck Maurin, Product and Solutions Director for Passenger Facilitation and Border Control, IDEMA

Jérémie Mella, Project Manager, AFNOR Certification

Michaël Mesure, Director LAF, SNCF

Jean-Michel Mis, Member of the French Parliament

Dana Rivera, Public Policy Manager at AWS, Amazon

Mathieu Rondel, Expertise & Operational Performance Director, Airport Operations Division, Groupe ADP

Frank Torres, Senior Director of Policy, Microsoft

Isabelle Valverde, Head of Flow Management, SNCF

Camille Vaziaga, Public Affairs Manager, Microsoft

Philippe Weiss, Head of Operations and Customer Vision, SNCF

We would also like to thank the French Data Protection Authority and the French Digital Council for their role as independent observers, and specifically:

Theodore Christakis, Member, CNNum

Karine Dognin-Sauze, Member, CNNum

Marie Duboys Fresney, Lawyer, CNIL

Salwa Toko, President, CNNum

Félicien Vallet, Engineer, CNIL

Lead authors

Sebastien Louradour, French Government Fellow, World Economic Forum

Lofred Madzou, Project Lead, AI and Machine Learning, World Economic Forum

Bibliography

- Castelluccia, Claude, and Le Métayer, Daniel, *Analyse des impacts de la Reconnaissance Faciale – Quelques éléments de méthode*, Inria Grenoble Rhône-Alpes, November 2019

- CNIL, *Facial Recognition: For a Debate Living Up to the Challenges*, November 2019

- Future of Privacy Forum, *Privacy Principles for Facial Recognition Technology in Commercial Applications*, September 2018

- German, Rachel, and Barber, K. Suzanne, *Current Biometric Adoption and Trends*, The University of Texas at Austin Center for Identity, September 2017

- Independent High-Level Expert Group on Artificial Recognition set up by the European Commission, *Ethics Guidelines for Trustworthy AI*, April 2019

- Li, Stan Z., and Jain, Anil K., *Handbook of Face Recognition*, Springer, March 2011

- Mitchell, Melanie , *Artificial Intelligence: A Guide for Thinking Humans*, Pelican, 2019

- OECD, *Artificial Intelligence in Society*, 2019

- OPECST, Didier Baichère, *La Reconnaissance Faciale, Les Notes Scientifiques de L'office*, July 2019

- Pew Research Center, *More than Half of U.S. Adults Trust Law Enforcement to Use Facial Recognition Responsibly*, September 2019

- West, Darell M., *10 Actions That Will Protect People from Facial Recognition*, Brookings website (www.brookings.edu/research/10-actions-that-will-protect-people-from-facial-recognition-software/), November 2019

Endnotes

1. “Facial Recognition Market Worth $7.0 Billion by 2024”, Markets and Markets, https://www.marketsandmarkets.com/PressReleases/facial-recognition.asp (link as of 28/1/20).

2. Patrick Grother, Mei Ngan and Kayee Hanaoka, “Ongoing Face Recognition Vendor Test (FRVT) Part 2: Identification”, NIST, https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8238.pdf (link as of 28/1/20).

3. “The Dawn of Robot Surveillance: AI, Video Analytics, and Privacy”, ACLU, https://www.aclu.org/report/dawn-robot-surveillance (link as of 28/1/20).

4. Nick Tabor, “Smile! The Secretive Business of Facial-Recognition Software in Retail Stores”, Intelligencer, 20 October 2018, http://nymag.com/intelligencer/2018/10/retailers-are-using-facial-recognition-technology-too.html (link as of 28/1/20).

5. Tom Simonite and Gregory Barber, “The Delicate Ethics of Using Facial Recognition in Schools”, Wired, 17 October 2019, https://www.wired.com/story/delicate-ethics-facial-recognition-schools/ (link as of 28/1/20).

6. Drew Harwell and Geoffrey A. Fowler, “U.S. Customs and Border Protection Says Photos of Travelers Were Taken in a Data Breach”, The Washington Post, 11 June 2019, https://www.washingtonpost.com/technology/2019/06/10/us-customs-border-protection-says-photos-travelers-into-out-country-were-recently-taken-data-breach/ (link as of 28/1/20).

7. Kashmir Hill, “The Secretive Company That Might End Privacy as We Know It”, 18 January 2020, https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html (link as of 28/1/20).

8. NISTIR 8280, Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf

9. “Facial Recognition: For a Debate Living Up to the Challenges”, CNIL, 15 November 2019, https://www.cnil.fr/sites/default/files/atoms/files/facial-recognition.pdf (link as of 28/1/20).

10. Claude Castelluccia and Daniel Le Métayer, “Analyse des impacts de la reconnaissance faciale – quelques éléments de méthode”, HAL-Inria, 2019, https://hal.inria.fr/hal-02373093 (link as of 28/1/20).

11. “EU Data Protection Rules”, EU website, https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018- reform-eu-data-protection-rules/eu-data-protection-rules_en (link as of 28/1/20).

12. “Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016”, EUR-Lex, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016L0680 (link as of 28/1/20).

13. Steven Shankland, “Tokyo 2020 Olympics Using Facial Recognition System from NEC, Intel”, CNET, 1 October 2019, https://www.cnet.com/news/tokyo-2020-olympics-using-facial-recognition-system-from-nec-intel/ (link as of 28/1/20).

14. David Oliver, “Facial Recognition Scanners Are Already at Some US Airports. Here’s What to Know”, USA Today, 18 August 2019, https://www.usatoday.com/story/travel/airline-news/2019/08/16/biometric-airport-screening-facial-recognition-everything-you-need-know/1998749001/ (link as of 28/1/20).

15. This process may vary depending on your data retention policy, the characteristics of the model used, the size of your organization and the nature of the contractual engagement between the procurer and user of the AI system.

WORLD
ECONOMIC
FORUM

COMMITTED TO
IMPROVING THE STATE
OF THE WORLD

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.

World Economic Forum
91–93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744
contact@weforum.org
www.weforum.org