44th Closed Session of the Global Privacy Assembly

October 2022

Resolution on Principles and Expectations for the Appropriate Use of Personal Information in Facial Recognition Technology

This Resolution is submitted by the sponsors on behalf of the International Enforcement Cooperation Working Group and the Ethics and Data Protection in Artificial Intelligence Working Group.

SPONSORS:

- European Data Protection Supervisor, European Union
- Federal Data Protection and Information Commissioner, Switzerland
- Information and Privacy Commissioner, Ontario (Canada)
- Information Commissioner's Office, United Kingdom
- Office of the Australian Information Commissioner, Australia
- Office of the Privacy Commissioner, Canada
- Personal Information Protection Commission, Japan

CO-SPONSORS:

- Catalan Data Protection Authority, Catalonia
- Commission for Informatics and Liberties, Burkina Faso
- Data Protection Authority, Netherlands
- Data Protection Authority, Norway
- Gibraltar Regulatory Authority, Gibraltar
- Information Access Commission, Quebec (Canada)
- Jersey Office of the Information Commissioner, Jersey
- National Access to Public Information Agency, Argentina
- National Commission for Informatics and Liberties, France
- National Privacy Commission, Philippines
- Office of the Information and Privacy Commissioner, Newfoundland and Labrador (Canada)
- Office of the Information and Privacy Commissioner, Nova Scotia (Canada)
- Office of the Privacy Commissioner, New Zealand
- Personal Information Protection Commission, Korea
- Superintendence of Industry and Commerce, Colombia

- Regulatory and Control Unit of Personal Data, Uruguay.

The 44th Annual Closed Session of the Global Privacy Assembly:

Recalling the Resolution on Facial Recognition Technology (FRT), adopted at the 42nd Closed Session of the Global Privacy Assembly (GPA) in October 2020, which highlighted the privacy risks of FRT and mandated the International Enforcement Cooperation Working Group (IEWG) and the Ethics and Data Protection in Artificial Intelligence Working Group (AIWG) to develop and promote a set of agreed principles and expectations for the appropriate use of personal information in FRT;

Recognising the establishment of a sub-group of IEWG and AIWG members and their efforts to deliver the mandate set out in the Resolution on FRT by: conducting research; carrying out a literature review; engaging the GPA membership; consulting with relevant global stakeholders; and developing the principles and expectations;

Acknowledging, following the adoption of the Resolution on FRT in October 2020, the continued development and deployment of live and retrospective FRT by public and private sector entities in a variety of settings such as: public spaces; work places; shops; educational settings; online; and in warzones;

Taking into account the ongoing global debate on FRT among a diverse set of stakeholders (including regulators, lawmakers, developers, users, academia and civil society), and their respective perspectives on the benefits and risks of FRT, set out in investigative findings, white papers, position papers, opinions, blogs, journal articles and other public communications;

Recognising the important contributions of data protection and privacy authorities, and international bodies, to the global debate, through publication of policy and guidance documents, including but not limited to:

- the European Data Protection Board's guidelines on the use of facial recognition technology in the area of law enforcement, and the EDPB-EDPS Joint Opinion on the EU Artificial Intelligence Act proposal;
- Canada's federal, provincial and territorial Privacy Commissioners' privacy guidance on facial recognition for police agencies;
- Canada's federal, provincial and territorial Privacy Commissioners' Recommended legal framework for police agencies' use of facial recognition;
- the UK Information Commissioner's Office's Opinions on the use of facial recognition technology in public places and the use of live facial recognition technology by law enforcement in public places;
- the Council of Europe's guidelines on facial recognition; and
- the United Nations Educational, Scientific and Cultural Organization (UNESCO)'s Recommendation on the ethics of artificial intelligence.

Highlighting the formal regulatory interventions and enforcement activity of data protection and privacy authorities, including undertaking investigations, and issuing fines, enforcement notices, cease and desist orders and recommendations in relation to deployment of FRT in a variety of settings by private sector, public sector, and law enforcement bodies.

Having regard to existing regulations and legislative developments covering use of FRT including: the Illinois Biometric Information Privacy Act, the European Union's proposed Artificial Intelligence Act, and Canada's proposed Artificial Intelligence and Data Act;

Appreciating the input of GPA members into the work of the FRT sub-group, by sharing their perspectives on the most significant privacy risks associated with specific uses of FRT;

Welcoming the input of FRT users, developers, lawmakers, and civil society organisations into the work of the FRT sub-group, by helping to refine the scope, terminology, clarity, coverage, and usability of the principles and expectations for the appropriate use of personal information in FRT;

Emphasising that compliance with data protection and privacy standards is vital for the responsible and trustworthy development and deployment of FRT, wherever in the world;

Reaffirming the commitments in the GPA's 2021-23 Strategic Plan to enhance the voice of the Assembly in digital policy, strengthen regulatory cooperation, and work towards a regulatory environment with high standards of data protection and privacy that are clearly and consistently applied across the world;

Recognising that the need for clear and consistent global data protection and privacy standards is especially important in the context of complex, high risk, technological innovations such as FRT, where benefits can be delivered, and differences in regulation may introduce uncertainty for stakeholders;

The 44th Global Privacy Assembly therefore endorses the principles and expectations for the appropriate use of personal information in facial recognition technology, summarised here and provided in full in the Annexe:

1. **LAWFUL BASIS**: Organizations using facial recognition should have a clear lawful basis for the collection and use of biometrics.

2. **REASONABLENESS, NECESSITY AND PROPORTIONALITY:** Organizations should establish, and be able to demonstrate, the reasonableness, necessity, and proportionality of their use of facial recognition technology.

3. **PROTECTION OF HUMAN RIGHTS:** Organizations should in particular assess and protect against unlawful or arbitrary interference with privacy and other human rights.

4. **TRANSPARENCY:** The use of facial recognition should be transparent to affected individuals and groups.

5. **ACCOUNTABILITY:** The use of facial recognition should include clear and effective accountability mechanisms.

6. **DATA PROTECTION PRINCIPLES:** The use of facial recognition should respect all data protection principles, including those referenced above.

The 44th Global Privacy Assembly resolves to work together in 2022-23 to:

1. Continue to deliver on the mandate in the GPA's 2020 Resolution on FRT by developing and implementing an engagement plan to:

    a. promote the principles with a range of key external stakeholder groups; and

    b. assess and review the real-world application of the principles by developers and users of FRT.

2. Request that the IEWG and the AIWG continue to work together to deliver this activity, and report back to the 45th Global Privacy Assembly Closed Session on their progress.

Annexe:

Principles and Expectations for the Appropriate Use of Personal Information in Facial Recognition Technology

Global Privacy Assembly

GPA
Global Privacy Assembly

Introduction

At the 42nd Closed Session of the Global Privacy Assembly (GPA) in October 2020, GPA members adopted a resolution on facial recognition technology (the Resolution).

The Resolution acknowledged that potential applications of facial recognition technology could provide benefits to security and public safety, but also highlighted that the technology has the capability to enable arbitrary or unlawful surveillance and the potential to be highly intrusive, provide biased results, and erode data protection, privacy, and human rights.

Public bodies, private organizations, and civil society have expressed concern that facial recognition technology poses privacy, legal and ethical challenges that must be addressed. At the same time, the GPA has previously identified the need to work towards global policy, standards and models for matters of significant privacy impact. This allows for greater levels of regulatory cooperation, enhances the efficient prevention, detection, and remediation of data protection and privacy issues, and ensures consistency and clarity in the system of oversight for the digital economy.

Thus, the GPA resolved to develop a set of agreed principles and expectations for the appropriate use of personal information in facial recognition technology, including recommending how risks can be mitigated. This document serves that purpose.

About Facial Recognition

Facial recognition is a process in which software tools analyze a digital image of an individual's face, extract their distinct features into a biometric template, and compare that template against one or more pre-extracted biometric templates. This can be done for the purpose of **verification** (e.g. a one-to-one comparison to verify an identity claim made by an individual) or **identification** (e.g. one-to-many or many-to-many comparison of an image of an unknown individual against a database of biometric references). It can occur in a variety of modes, including **live** or **near-live** applications (e.g. real-time comparison of one or more faces against a watchlist) and **retrospective** applications (e.g. comparison of a previously captured image of an unknown individual against a database of biometric references, such as during a police investigation).

As acknowledged in the Resolution, facial recognition technology relies on sensitive biometric information that is unique to the individual and difficult to alter. Decisions made about individuals using these identifiers, often without their knowledge or consent, can lead to adverse consequences without appropriate avenues for recourse. In addition to impacts on privacy, the widespread use of facial recognition can also lead to discriminatory effects and impact the ability to exercise other fundamental human rights, such as the freedom of expression, movement and association.

Application of the Principles

These principles apply to all types and uses of facial recognition by both private and public sector (including law enforcement) organizations. While for ease of reference we have used

the term “facial recognition” throughout this document, the principles set out below apply equally to any biometric analysis of facial images and biometric templates (such as inference of demographic characteristics, emotional state, etc.). The principles are intended to apply to users, developers and suppliers of facial recognition systems.

Importantly, the principles set out below are of equivalent importance and should be considered holistically.

Lastly, we acknowledge that governments and data protection regulators have an important role in facial recognition technology, particularly with respect to establishing and enforcing appropriate regulatory frameworks. However, that is out-of-scope for this document.

Terminology

In this document we have used the following terms:

> **Biometric**: A biometric is a measurement of a physiological feature (e.g. a person’s fingerprint, iris, face or hand geometry) or behavioural attribute (e.g. gait or keystroke pattern) of an individual. These characteristics are mostly persistent, unique to the individual, and difficult or impossible to change (i.e. changing a biometric requires a change to the individual’s physical person). As such, they should be considered sensitive.
>
> **Biometric template**: A digital or mathematical representation of an individual’s biometric. Though the specific template format is changeable, it represents a characteristic that is unique, difficult to alter, and inseparably linked to a person; as such, it should be treated as sensitive.
>
> **Biometric probe**: A biometric template extracted from an image of an unknown or unverified individual, which will be compared against a biometric reference (in the case of verification) or a reference database (in the case of identification).
>
> **Biometric reference**: A biometric template extracted from an image associated with a known identity, against which a biometric probe is compared.
>
> **Reference database**: A list or database of biometric references, against each of which a biometric probe is compared.

Legal Consideration

The principles below are phrased as recommendations (using the term “should”). However, many of them are explicit statutory requirements in members’ jurisdictions or may be interpreted as such by courts and data protection authorities. It is incumbent on any organization seeking to use facial recognition technology to understand the applicable legal requirements within their jurisdiction.

PRINCIPLES

1. LAWFUL BASIS: Organizations using facial recognition should have a clear lawful basis for the collection and use of biometrics.

1.1. Organizations should document, and be prepared to demonstrate, the lawfulness of their use of biometrics for facial recognition. This includes both the lawful basis for capturing an image of an individual to create a biometric probe, and for creating, accessing or amending any reference database that is, or will be, used. This should be periodically reassessed to account for changes in law or its interpretation.

1.2. If operating in a jurisdiction which recognizes multiple lawful bases for processing, organizations should consider whether another basis is more appropriate than consent. In many applications, including use of facial recognition in publicly accessible spaces and employment contexts, it may be challenging for an organization to demonstrate that it has obtained meaningful consent from an individual.

1.3. If consent is the basis for processing, organizations should ensure and be able to demonstrate that consent is meaningful. This means that it is informed, specific, current, freely given, and unambiguous. This includes consideration of an individual's capacity to provide meaningful consent (such as in the case of youth or vulnerable persons).

> 1.3.1. Express consent is preferred. Organizations should be aware that implied consent would not meet the standard for consent in many jurisdictions, and in general should not be relied on for collection of sensitive personal information. However, should a situation arise in which an organization considers they can rely on implied consent for facial recognition, they should be able to demonstrate that it is (i) appropriate in the circumstance, and (ii) reasonable to believe in the circumstance that an individual has consented.

1.4. Organizations should be aware that in many jurisdictions, scraping of images from publicly accessible online platforms (including from social networking services) to create a facial recognition reference database is not considered to be lawful or fair, nor is it considered to be a transparent process.

2. REASONABLENESS, NECESSITY AND PROPORTIONALITY: Organizations should establish, and be able to demonstrate, the reasonableness, necessity and proportionality of their use of facial recognition technology.

2.1. Organizations should establish the necessity of using facial recognition technology. Given the sensitivity of the information involved, the threshold for establishing necessity is high. It requires clearly establishing the intended purpose, that facial recognition technology can be effective in achieving this purpose, and that the purpose cannot reasonably be achieved by less intrusive means. Convenience or desirability should not be relied upon to establish necessity.

2.2. Organizations should establish, and be able to demonstrate, the proportionality of their use of facial recognition technology. Again, the threshold for establishing proportionality is high. The benefits of the use of facial recognition should clearly outweigh the risk of harm it poses to individuals' privacy and other human rights. In establishing proportionality:

2.2.1. Organizations should document, and be able to demonstrate, the benefits expected from the use of facial recognition technology. Organizations should also clearly define how they will measure whether the system has realized these benefits, and the level of benefit below which the use of facial recognition would be ceased.

2.2.2. Organizations should document, and be able to demonstrate, that they have assessed potential or known risks of harm posed by their proposed use of facial recognition. This should include consideration of the risks of harm to individuals and to groups. Organizations should also clearly document the measures that they have implemented to mitigate identified risks.

2.2.3. In the case of identification, an organization should demonstrate a clear public interest in the use of the technology. In general, commercial gain will not by itself be considered to be a clear public interest.

2.2.4. The threshold for proportionality may be more easily met in cases of use of facial recognition technology for verification where the organization can show that individuals have meaningfully consented to the use of the system as set out in Principle 1.3.

2.3. Organizations should establish the reasonableness of their use of facial recognition technology. The threshold for establishing reasonableness is high. What is reasonable is a question of fact in each individual case. Reasonableness can be influenced by community expectations, as well as current standards and practices of facial recognition technology.

2.4. To avoid decisions being influenced by sunk costs or commitments, the assessment of reasonableness, necessity and proportionality should be undertaken in advance of the purchase, development or deployment of a facial recognition system.

2.5. Organizations should be aware of any determination from their respective data protection authorities that the known or potential harms of certain application(s) of facial recognition are so substantial that they cannot be proportional to the intended benefits.

2.5.1. In particular, organizations should be aware that the potential harm associated with the recognition of human features in publicly accessible spaces (including by facial recognition) has led multiple national, regional and local data protection authorities, including all EEA data protection authorities, to propose bans on the practice.

2.5.2. Organizations should also be aware that many data protection authorities have called for a ban on other forms of facial analysis not related to verification and identification, such as the inference of emotional state.

2.6. An organization's assessment of reasonableness, necessity and proportionality should be regularly re-visited. This should include consideration of, among other things, whether the need being addressed still exists; whether the expected benefits from the use of facial recognition were realized; and whether any previously unidentified harms arose, or any identified harms were worse than anticipated, such that those harms now outweigh the benefits.

3. PROTECTION OF HUMAN RIGHTS: Organizations should in particular assess and protect against unlawful or arbitrary interference with privacy and other human rights.

3.1. In general, organizations should assume that the use of facial recognition technology may unduly interfere with individuals' data protection and privacy rights.

> 3.1.1. This interference is generally greatest when using these technologies in a publicly accessible space. Organizations should take particular note that an individual's presence in a public location does not necessarily mean that they have forgone any reasonable expectation of privacy or control of personal information. Per Principle 2.5.1, multiple data protection authorities have proposed bans on such uses.
>
> 3.1.2. Interference will also be heightened by any use of facial recognition which tracks an individual's movements, actions or behaviours over time (in the same or multiple locations and, in particular, locations that may reveal sensitive information about a person).

3.2. Organizations should not assume that images of individuals that are publicly accessible on the Internet (including on social media sites) can be collected and transformed for use as biometric probes or biometric references, or to train a facial recognition system, without the knowledge and consent of those individuals or another lawful basis for such collection and use.

3.3. When determining potential impacts on data protection and privacy rights, organizations should:

> 3.3.1. Undertake appropriate impact assessments (such as a Privacy Impact Assessment, Data Protection Impact Assessment or Human Rights Impact Assessment).
>
> > 3.3.1.1. Organizations should be transparent to all potentially affected individuals about their assessment and mitigation of privacy risks.
>
> 3.3.2. Consider demographic differentials (i.e. bias) with respect to both the functioning of the system (e.g. relevant performance differences across groups) and application of the system (e.g. differences in how the deployment of the system will impact individuals or groups). Organizations should also consider how they will measure, on an on-going basis, any differential impacts across groups of use of the facial recognition system.

3.3.3. Consider the potential "chilling effect" on rights such as freedom of expression and freedom of association, and the potential for discrimination, connected with the use of facial recognition systems in publicly accessible spaces, regardless of the intended purpose of those systems.

3.3.4. Where marginalized groups may be particularly impacted by the use of a system, consult with representatives from those groups about the anticipated impacts and strategies to reduce harms.

3.4. Where possible, when using facial recognition for verification an alternative method that does not rely on biometrics should be made available, including for those individuals who refuse or withdraw consent. Individuals should not be penalized for the use of this alternative.

4. TRANSPARENCY: The use of facial recognition should be transparent to affected individuals and groups.

4.1. Organizations should ensure that individuals are informed (in plain language) of:

4.1.1. Any time that their captured facial image may or will be subject to a facial recognition system, or that their biometric template may or will be included in a reference database for a facial recognition system. It is preferable and best practice – and in some circumstances, required by law – for individuals to be notified of this before, or at the time that, their facial image is captured.

4.1.2. Their data rights with respect to facial recognition systems, as well as how to exercise them. This includes but is not limited to the ability to request that their facial image not be subject to a facial recognition system, that their biometric template be deleted from a reference database (if applicable), or that information about them in a facial recognition system be corrected (e.g. by updating their biometric reference).

4.1.3. Any other information required to be provided to individuals by law in their jurisdiction. This includes how and where information will be stored, for what purposes it will be processed, how long it will be retained, and with what entities it may be shared.

4.2. Organizations should consider how they will ensure adequate notice is provided to all individuals, including youth and vulnerable persons.

4.3. Organizations should be aware that signage about the use of a facial recognition system will generally not, by itself, be sufficient for compliance with Principle 4.1.

4.3.1. Where consent is relied on for processing, and signage is an element of this consent process, signage should be prominently visible before an individual enters a surveilled area. This signage should include an indication of any available alternatives for accessing the space. Signage should also clearly indicate that facial recognition is in use, as opposed to a standard security camera.

4.3.2. Where signage is a key part of an organization's notice strategy, consideration should be given to how notice will be provided to those who may have difficulty reading or understanding the signs.

4.4. In the case of retrospective facial recognition, organizations should take proactive steps to ensure individuals are made aware of the use and purpose of the system. This includes both publication of this information in advance of use of the system, as well as (whenever reasonable) specific notice to individuals whose images have been processed by the system.

5. ACCOUNTABILITY: The use of facial recognition should include clear and effective accountability mechanisms.

5.1. Organizations should establish clear governance and risk mitigation policies for all uses of facial recognition, and be prepared to demonstrate the existence and effectiveness of these policies.

5.1.1. Organizations should establish and maintain a means of detecting non-compliance with governance and risk management policies for facial recognition (including by internal actors), and consequences for non-compliance.

5.2. All users of a facial recognition system should undertake regular training on any relevant internal privacy policies, the legal requirements in their jurisdiction, the limitations and potential biases of facial recognition systems, how to conduct facial comparison, and ways to mitigate known risks such as automation bias (i.e. the tendency for humans to give greater weight to suggestions made by an automated system).

5.3. Wherever reasonable, conclusions reached about the identity of an individual should be assessed by a human who has undertaken relevant training. This is particularly the case where an individual will be significantly affected by such a conclusion.

5.3.1. Individuals should be provided the opportunity to challenge, and seek redress for, any decision made about them based on an identification using facial recognition.

5.3.2. Organizations should ensure that the threshold for a 'match' is reasonable for the proposed application of the system, whether this threshold is determined by the organization itself or by the developer of the system.

5.3.3. Organizations should establish mitigation strategies to manage risks associated with mismatches (both false positives and false negatives) and mis-registration (i.e. inaccuracies in the reference database).

5.4. Organizations should recognize the limitations of facial recognition systems and interpret outputs produced by those systems accordingly. For instance, in the context of a retrospective facial recognition system used by law enforcement, a 'match' should be considered a potential lead as opposed to conclusive or admissible evidence.

5.5. Organizations should undertake periodic audits of the effectiveness of the facial recognition system, risk mitigation measures put in place, and internal compliance with governance policies.

5.6. Organizations should monitor and regularly evaluate any demographic differentials in the effectiveness of their use of a facial recognition system.

5.7. Organizations developing facial recognition systems should document the steps taken to measure and protect against demographic differentials in their products, as well as the effectiveness of these measures (i.e. any known performance differences across demographic groups).

5.8. Organizations looking to purchase or otherwise use facial recognition systems should:

> 5.8.1. Obtain information about the measurement of and protections against demographic differentials documented per Principle 5.7.
>
> 5.8.2. Obtain information about the demographics of the training, testing and evaluation datasets of the product, to ensure that they have included a sufficiently diverse range of individuals for the intended context.
>
> 5.8.3. Ensure that the product was designed for and tested in a way that is compatible with the intended use. For instance, a facial recognition product designed for verification in a well-lit, controlled environment may not be sufficiently accurate for identification in a dark, high-angle or highly dynamic setting (i.e. moving crowd).
>
> 5.8.4. If relying on a third-party service provider, have in place a robust vendor risk management framework for assessing compliance with principle 5.10, as well as associated contractual protections to ensure compliance will be on-going.

5.9. Organizations should establish procedures and policies for identifying, mitigating, responding and notifying the relevant data protection authority of any data breaches relating to the facial recognition system.

5.10. Organizations should ensure that any third parties they engage meet the Principles set out in this document (to the extent that they apply to the third-party), as well as any legislative requirements.

6. DATA PROTECTION PRINCIPLES: The use of facial recognition should respect all data protection principles, including those referenced above.

Organizations must consider *all* data protection principles throughout the lifecycle of a facial recognition system. In addition to those described above, these include:

6.1. Privacy by design.

> 6.1.1. When developing a facial recognition system, organizations should adopt a privacy by design approach to ensuring protections are built into facial recognition systems from the outset.

6.1.2. Where reasonable, organizations should avoid central storage of biometric templates and any raw biometric data. For example, in the case of verification, the biometric reference could be stored on a device or artifact (such as a driver's license, passport, or employee identification badge) held by the individual being verified. If biometric templates are centrally stored (where specific purposes for doing so are identified), they should be protected by strong and appropriate cryptographic measures.

6.1.3. Organizations using a facial recognition system should ensure appropriate safeguards are applied throughout each stage of the system's information lifecycle.

6.2. Purpose specification and use limitation.

6.2.1. Organizations should clearly define the purposes for which facial recognition systems will be used, and not vary from those purposes unless legally permitted.

6.3. Data Minimization, Retention, and Deletion.

6.3.1. Organizations should define retention periods for raw biometric data and biometric templates (including those used as biometric probes or biometric references, or stored in reference databases), and delete biometric templates when it is no longer necessary to retain them. This period should take into account the decreasing usefulness of a biometric template over time.

6.3.2. In general, biometric probes that do not match against a biometric reference should be deleted immediately. Limited retention of such images may be acceptable if reasonably necessary, such as for system testing which has a clear legal basis and is in line with the defined purpose for the processing in question, where an appropriate retention policy is in place. Matched biometric probes may be retained for a specified period, but should only be used in relation to that match (i.e. for evidentiary purposes, or to permit individuals to challenge a decision made about them).

6.3.3. Unless necessary for a defined (and lawful) purpose, organizations should avoid creating a profile of an individual's activities or behaviours by correlating facial recognition matches across time.

6.3.4. Organizations should have in place accessible mechanisms for individuals to seek removal of their biometric template from a reference database when they no longer consent to their inclusion, or they have other lawful grounds for seeking and obtaining removal. Such removals should be expedient, taking place as soon as possible (and within any legally defined timelines).

6.4. Safeguards.

6.4.1. Organizations should implement security safeguards proportionate to the high sensitivity of the information in a facial recognition system.

6.4.2. Organizations should implement the necessary policies, procedures, security standards and controls to ensure that neither the facial recognition system nor the personal information it collects or stores is subject to unauthorized or unintentional access, misuse, interference, or loss.

6.4.3. Organizations should ensure any facial recognition systems they are deploying (including those developed by third parties) include appropriate biometric template protection measures, and that these protections are in use. Where possible, these should conform to internationally recognized standards for protection of biometric information.

6.4.4. Organizations should regularly review their security safeguards to ensure they remain sufficient for an evolving threat landscape.

6.5. Data Quality.

6.5.1. Organizations should ensure that biometric references, and any other personal information collected, generated and stored by the facial recognition system, are sufficiently accurate and up-to-date for the purpose for which they are being used.

6.5.2. Organizations should take reasonable steps to correct or delete any personal information that are inaccurate in relation to the purpose for which they are being used.

6.5.3. Organizations should ensure that only images well-suited for use with facial recognition systems are included in biometric reference databases or used as biometric probes. Quality assessments should at least take into account image characteristics including pose, illumination, expression, image size and resolution, and facial occlusion (i.e. the presence of eyeglasses, hats, scarves, or masks).