# Provisions on Security Management in the Application of Facial Recognition Technology (Trial) (Draft for Comment)

by China Law Translate | 2023/08/08 9:27 AM

**[Source]**http://www.cac.gov.cn/2023-08/08/c_1693064670537413.htm

**Article 1:** These Provisions are drafted on the basis of the Cybersecurity Law of the PRC, the PRC Data Security Law, the Personal Information Protection Law of the PRC, and other laws, so as to regulate the use of facial recognition technology, protect rights and interests in personal information and other rights and interests in persons and property, and maintain social order and public safety.

**Article 2:** Those using facial recognition technology to handle facial information or providing facial recognition technology goods and services within the [mainland territory of the] People's Republic of China shall abide by these Provisions. Where laws or administrative regulations provide otherwise, follow those provisions.

**Article 3:** The use of facial recognition technology shall comply with laws and regulations, comply with public order, respect social mores, bear social responsibility, and fulfill obligations to protect personal information; facial recognition technology must not be used to engage in activities that are prohibited by laws and regulations, such as those that endanger national security, harm the public interest, disrupt social order, or infringe the lawful rights and interests of individuals and organizations.

**Article 4:** Facial recognition technology may only be used to handle facial information where there are specified purposes and sufficient need, and where strict protective measures are employed. Where other non-biometric identification schemes exist that can realize the same goals or achieve the same operational requirements, priority shall be given to the non-biometric identification schemes.

Where facial recognition technology is used to verify personal identities or to identify specified natural persons, giving priority to the use of authoritative channels such as the National Database of Basic Population Information and the National Online Identity Authentication Public Service is encouraged.

**Article 5:** Individuals' specific consent shall be obtained, or written consent obtained in accordance with law, for the use of facial recognition technology to handle facial information. Except where laws and administrative regulations provide that it is not necessary to obtain the individuals' consent.

**Article 6:** Image acquisition and personal identification equipment must not be installed in locations that might infringe on others' privacy, such as hotel rooms, public bathhouses, dressing rooms, and bathrooms.

**Article 7:** The installation of image acquisition and personal identification equipment in public places shall be as necessary to preserve public safety, shall comply with relevant national regulations, and have prominent notifications in place.

The units that establish, use, operate, and maintain image acquisition and personal identification equipment in public places have an obligation to preserve the confidentiality of personal images and identification information that is collected, and must not illegally disclose it or provide it externally. The collected personal images and identification information can only be used for the purpose of preserving public safety, and must not be used for other purposes unless the individual's specific consent is obtained.

**Article 8:** Where organizations install image acquisition and personal identification equipment in order to carry out internal management, they shall reasonably determine the area for image and information acquisition, employ strict protection measures, and prevent conduct such as illegally accessing, reproducing, disclosing, externally providing, or transmitting personal images, and preventing the disclosure, alteration, and loss of personal information, or its being illegally acquired or used.

**Article 9:** Hotels, banks, bus stations, airports, stadiums, exhibition halls, museums, art museums, libraries, and other such business locations must not force, mislead, trick, or coerce individuals into accepting personal identity verification through facial recognition technology on grounds such as handling operations or improving service quality, except where laws and administrative regulations provide that facial recognition technology shall be used to verify personal identities.

Where individuals voluntarily select to use facial recognition technology for identity verification, it shall be ensured that the individual is fully informed and actively participating, and clear notice of the purpose of the identity verification shall be immediately given during verification through means such as explicit and understandable speech or text.

**Article 10:** The use of facial recognition technology for long-distance, frictionless identification of specific natural persons in public places and business premises shall be in order to preserve national security and public safety, or as needed in emergency situations to protect natural persons' lives and health or the safety of property, and be proposed by the individual or a stakeholder.

Those using facial recognition technology for remote and frictionless identification of specific individuals or stakeholders at the request of the individual or stakeholders, shall limit the relevant services to the smallest necessary time, place, and group of people, and must not associate them with personal information that is not directly and inherently related to the request.

**Article 11:** Organizations and individuals must not use facial recognition technology to analyze individuals' race, ethnicity, religious beliefs, health status, social class, or other sensitive personal information, except to maintain national security and public safety or as necessary in emergency situations to protect natural persons' lives and health and the safety of property, or where specific consent is obtained.

**Article 12:** Where major interests such as social assistance or the disposition of real property are involved, facial recognition technology must not be used in place of human review of

individuals' identities, but facial recognition technology may be a supplemental method of identity verification.

**Article 13:** Those using facial recognition technology to handle the facial information of minors under the age of 14 shall obtain the specific or written consent of the minors' parents or other guardians.

The parents or other guardians of minors shall correctly perform guardianship duties, teaching and guiding minors under the age of 14 to strengthen their awareness and ability to protect personal information.

**Article 14:** Property service enterprises and other building managers must not make the use of facial recognition technology for identity verification the only means of entering or exiting the managed area, and where individuals do not consent to identity verification by facial information, the property service enterprises or other building managers shall provide other reasonable and convenient means for verifying their identities.

**Article 15:** Those using facial recognition technology to handle facial information shall first conduct an assessment of the impact on personal information protection and make a record of the handling.

Personal information protection impact assessment reports are to primarily include the following content:

(1) Whether the provisions of laws and administrative regulations, and the mandatory requirements of state standards are met, and whether it meets ethics and morals;

(2) Whether there is a specified purpose and sufficient necessity for the handling of facial information;

(3) whether it is limited to the accuracy, precision, and distance requirements necessary to achieve the purpose;

(4) Whether the protection measures employed are legal, effective, and correspond to the degree of risk;

(5) The risks of disclosure, alteration, loss, or destruction of facial information, or of its being illegally obtained or used, as well as the harm that might be caused;

(6) The potential harm and impact to personal rights and interests, as well as whether measures for reducing the adverse impact are effective.

Personal information protection impact assessment reports should be retained for at least three years. Where there is a change in the purpose or methods of handling facial information, or there is a major security incident, the users of facial recognition technology shall newly conduct a personal information protection impact assessment.

**Article 16:** Users of facial recognition technology that use it in public locations or that store more than 10,000 people's facial information, shall file with the prefecture-level internet

information department within 30 working days. Applications for filings shall submit the following materials;

(1) The basic circumstances of the facial recognition technology users and their person responsible for personal information protection;

(2) An explanation of the necessity of handling facial information;

(3) The purpose and methods of handling facial information and the safety and protection measures;

(4) The rules and processes for handling facial information;

(5) The personal information protection impact assessment report;

(6) Other materials that the internet information departments feel there is a need to provide.

Where facial recognition technology users handle facial information and there are laws and administrative regulations providing that it shall be kept secret, is to be implemented in accordance with the relevant provisions.

Where there are substantive changes to filing information, the filing modification procedures should be completed within 20 working days of the change. Where the use of facial recognition technology is concluded, de-registration procedures for the filings should be handled within 30 working days of the conclusion.

**Article 17:** Those using facial recognition technology must not save original images, pictures, or videos of faces other than in the legally-prescribed conditions or on obtaining the individuals' specific consent, except where the face information has been anonymized.

Where facial recognition technology services are provided to the public, the technology system shall comply with the requirements of level 3 or higher network security protections, and employ measures such as data encryption, security audits, access controls, authorization management, intrusion testing, and defenses to protect the security of facial information. Where it is critical information infrastructure, the requirements related to security protection for critical information infrastructure shall also be met.

**Article 18:** In the use of facial recognition technology to handle facial information, the collection of facial information unrelated to the provision of services shall be avoided as much as possible, and where it is unavoidable, it shall be promptly deleted or anonymized.

**Article 19:** Those using facial recognition technology shall conduct testing and assessments annually of the security and potential risks of image acquisition and personal identification equipment, improve their security strategy based on the testing and assessments, adjust the confidence thresholds, and employ effective measures to protect the image acquisition and personal identification equipment from attacks, incursions, disruptions, and destruction.

**Article 20:** Image acquisition and personal identification equipment that is listed in the directory of critical network equipment and specialized network security products in accordance with relevant State provisions shall follow the mandatory requirements in state

standards, and may only be sold or provided after it has been certified by a qualified institution or tested as meeting requirements.

**Article 21:** Based on their duties and in conjunction with relevant departments such as telecommunication departments, public security organs, and market administration departments, the internet information departments are to strengthen oversight inspections over those using facial recognition technology, guiding and urging them to perform filing procedures, and promptly discovering security threats and urging their rectification in a set period of time.

Those using facial recognition technology or providing facial recognition technology products or services shall cooperate with oversight inspections carried out by relevant departments in accordance with law.

**Article 22:** Where any organization or individual discovers conduct violating these Provisions, they may make a complaint or report it to the relevant departments such as for internet information, telecommunications, public security, or market administration.

Where relevant departments such as for internet information, telecommunications, public security, or market administration receive complaints or reports, they shall make a disposition in accordance with law on the bases of their duties.

**Article 23:** Where those using facial recognition technology or providing facial recognition technology products or services violate these Provisions, penalties are to be given by relevant departments such as for internet information, telecommunications, public security, or market administration within the scope of their duties in accordance with the provisions of the PRC Cybersecurity Law, The PRC Data Security Law, the PRC Law on the Protection of Personal Information, and other such laws and administrative regulations. Where the Public Security Administration Punishments Law is violated, public security administrative punishments are to be given in accordance with law; and where a crime is constituted, criminal responsibility is to be pursued in accordance with law

Where violations of these Provisions cause harm to others, civil liability is to be borne in accordance with law.

**Article 24:** The Cybersecurity Administration of China, in conjunction with the Ministry of Industry and Information, Ministry of Public Security, and State Administration for Market Regulation, is responsible for interpreting these Provisions.

**Article 25:** These Provisions are to take effect of XX/XX/XXXX.