DS NEWSLETTER Savoir Faire

NEWSLETTER - LEGAL INFORMATIONS

PROPOSED BY DS AVOCATS

Should we fear facial recognition?

ASIA

BACKGROUND

Facial recognition is a technology combining biometric techniques, artificial intelligence, 3D cartography and Deep Learning to compare and analyze human features in order to identify a person. It uses cameras to collect images or video stream, and then automatically detect the facial data within them to achieve facial recognition.

Over the last 3 years, facial recognition has been widely used in various fields such as finance, justice, military, public safety, border control, government utility, aerospace industry, power sector, manufacturing industry, education, medical, private and public companies and public institutions. Thus, for example, it is generally used to access applications on mobile phones. In fact, it allows us to make online payments and log onto certain bank accounts by merely "smiling" at the camera of our mobile phones. With the increasing popularity of this technology, facial data is gradually becoming the access key and new password to bank accounts.

In recent years Chinese authorities have published several circulars or notices advocating for the application of facial recognition technology. Therefore, facial recognition increasingly plays a role in our daily lives:

- The People's Bank of China encourages, since November 2016, Chinese banks to employ safe and effective technological means to verify personal identity data of individual bank account holders. In accordance with this principle, several banks use facial recognition to verify the identity of bank account holders.
- In Fujian province and Guangzhou city, retired people can file their retirement and pension access applications by facial recognition, which facilitates administrative formalities
- The Local Taxation Office in Beijing has started to issue duty-paid certificate/proof for expats, using facial recognition.
- The Council of State Affairs recommended in a circular on February 26, 2019, the implementation of facial recognition in order to improve the "Internet-based Real Estate Registration".

In addition to all mentioned implementations, numerous office buildings, road safety barriers and mobile applications use facial recognition.

GENERAL LEGAL CONTEXT

Facial recognition, is a sensitive subject as it involves the collection and recognition of strictly personal data, specifically facial biometrics Its misuse can have a real impact on our private life Therefore, given for the potential threats to our private lives linked to technological abuse, some countries like the USA, China and Sweden have started to restrict or even forbid the use of facial recognition technology in certain fields.

You might have heard that in July of 2019, the US Federal Trade Commission sanctioned Facebook of a USD 5 billion fine for abuse of facial recognition technology. As a result of this fine, Facebook has updated its facial recognition function, which is no longer enabled by default, and from now on users are able to choose their own settings.

Similarly, in China, on November 1st, 2019, there has been a complaint regarding an abuse of facial recognition technology filed in Hangzhou City Fuyang District People's Court. The plaintiff, an annual card holder of a zoo, sued the zoo because it changed the entrance system from scanning fingerprints to using facial recognition without consultation and without annual card holders' prior consent. The zoo was then charged for violation (i) of the relevant service agreement between the zoo and its annual card holders and (ii) of the PRC Law of Protection of Consumer Rights and Interests.

GENERAL PRINCIPLES OF THE PROTECTION OF BIOMETRIC DATA INFORMATION IN CHINA

Facial recognition is based on the biometric information of private persons, which is clearly defined as personal data* and protected by

The Newsletter is provided for general informational purposes only. Any information contained in this should not be construed as legal advice and is not intended to be a substitute for legal counsel on any subject.

Chinese laws according to item 5 Article 76 of the PRC Cyber Security Law ("CSL").

CSL further stipulates that network operators should follow the principles of legality, proportionality and necessity when collecting and using personal data and thus biometric information. In addition, they should indicate the purpose, the method and the scope of collecting and the usage of the data.

The main requirements under CSL regarding collecting and using of facial data are as follows:

Requirements	Contents
Clear notification	Network operators shall not use vague expressions to obtain consent from private persons.
Express consent	Network operators must obtain private persons' express consent instead of implied consent.
Relevance	Network operators are not allowed to collect personal data which is irrelevant to their business activities.
Confidentiality	Network operators shall not divulge or alter the personal data they collect, or provide personal data to any third parties without prior consent of the private persons concerned, except when personal data has been processed in such way that it cannot be recovered or matched with a specific person, hence confidentiality of personal data is maintained.
Right to deletion/correction	Private persons have a right to ask for correction and/or deletion of their personal data to network operators; and they must take measures to delete or correct such data.
Administrative penalties for violation of any of the above 5 requirements: • Warning and/or; • Confiscation of illegal gains and/or; • Fine of no less than one but no more than ten times the illegal gains; • Where there is no illegal gain, a fine of less than RMB 1 million shall be imposed; • A fine of no less than CNY10,000 (around EUR 1,278) but no more than CNY100,000 (around EUR 12,776) can be imposed on the persons directly responsible; • Where the circumstances are serious, the network operators can be ordered to: - suspend relevant business - stop their business activities for rectification - close down their website - have their relevant business permits or their business licenses revoked.	

All information recorded electronically or by any other means which can be used independently or jointly to identify personal information of a private person including non-exhaustively – names, date of birth, identity card number, biometric information, addresses, telephone number etc.

The Newsletter is provided for general informational purposes only. Any information contained in this should not be construed as legal advice and is not intended to be a substitute for legal counsel on any subject matter.

Illegal use of personal data is prohibited	It is not allowed to acquire personal data by stealing or through other illegal ways, nor illegally sell or provide personal data to others.
Administrative penalties for violation of the above obligation: • Confiscation of illegal gains and/or; • Fine of no less than one but no more than ten times the illegal gains; Where there is no illegal gain, a fine of less than RMB 1 million (around EUR 128,000)	

ADDVICES OF DS:

In addition to satisfying the "prior consent" principle, considering that facial data contains higher data security risk, companies should carefully evaluate whether the usage follows the principle of "legality, proportionality and necessity". For instance, is it really necessary to collect face recognition data to check attendance, counting and other purposes? Is there any alternative way which can achieve the same purpose by collecting other type of data with relatively low sensitivity?

Besides, companies must take reasonable measures to restrict access to collected data and respect minimal necessary and reasonable demands during data retention period.

Where the facial data obtained by a company is subsequently used for other commercial purposes, it is necessary to duly inform the concerned individuals and have their consent in advance. In addition, companies shall take reasonable measures to prevent access to the data whether authorized or not, and to avoid collecting unnecessary type and/or volume of data. As for the retention time (for how long the personal data can be held and/or controlled since it has been collected), currently there is no unified and mandatory maximum retention time regarding personal data, normally the retention time cannot exceed the necessary length of time required by the commercial needs and/or relevant laws and regulations. However, please note that for some special fields there is mandatory minimum retention time related to personal data. For example, CSL requires network operators to preserve relevant web logs regarding the network operation status and cyber security incidents for no less than six months. In this case, if such web logs include personal data, they shall be preserved for at least 6 months by the network operator.

In case of using the face recognition software and equipment and facilities provided by the third party, it is highly recommended to enter an agreement with such third party to define the scope of use of personal sensitive data, the rights and obligations of the parties, confidentiality obligations, retention time of personal sensitive data and the private persons' right to be forgotten at the termination of business cooperation. For example, if company A collects personal data (may include facial data) by software provided by company B, and these two companies have entered into an agreement as mentioned above, company A may need to inform company B to delete certain personal data saved/shared with company B by company A upon these two companies end cooperation or upon request by the concerned individual.

Finally, based on currently applicable laws and regulations, facial data is not clearly defined as being part of the personal sensitive data category. According to the Information Guide about information security and personal information protection of the information system for public and commercial services, personal sensitive data refers to personal information which can have negative effects if they are disclosed or modified. These include for example, identity card numbers, origin, political affiliation, religion or personal beliefs, genetic information or fingerprints etc.

It is also worthwhile to note that, in the near future the facial data might be clearly specified as personal sensitive data. Per the National Standard Entitled Data Security Technology - Personal data Security Specifications (Draft version seeking comments), facial data is considered as individual biometric data under

The Newsletter is provided for general informational purposes only. Any information contained in this should not be construed as legal advice and is not intended to be a substitute for legal counsel on any subject matter.

the type of personal sensitive data. In this case, companies will need to undertake stricter security protection obligations for such data. Therefore, companies should continue to improve their safety protection of biometric data, take encryption protection measures, isolation storage, use after desensitization (desensitization refers to processing the personal data so that it cannot be used to identify a specific individual) and other technical measures, and should implement timely and thorough destruction of data when there is no more need for processing or the person concerned ask for its deletion.

For any additional information please contact:

Zhang Beibei : Associate
zhangbeibei@dsavocats.com

Sylvie Savoie : Counsel
savoie@dsavocats.com

The Newsletter is provided for general informational purposes only. Any information contained in this should not be construed as legal advice and is not intended to be a substitute for legal counsel on any subject matter.