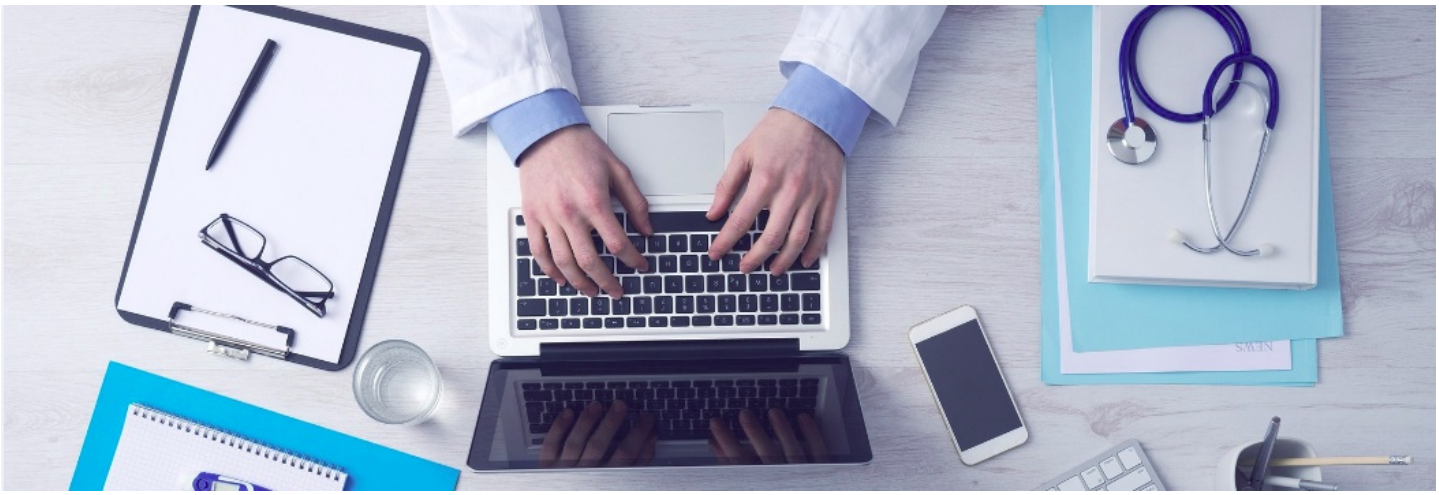
The use of automated facial recognition technology and supervision mechanism in UK



The use of automated facial recognition technology and supervision mechanism in UK

I. Introduction

Automatic facial recognition (AFR) technology has developed rapidly in recent years, and it can identify target people in a short time. The UK Home Office announced the "Biometrics Strategy" on June 28, 2018, saying that AFR technology will be introduced in the law enforcement, and the Home Office will also actively cooperate with other agencies to establish a new oversight and advisory board in order to maintain public trust. AFR technology can improve law enforcement work, but its use will increase the risk of intruding into individual liberty and privacy.

This article focuses on the application of AFR technology proposed by the UK Home Office. The first part of this article describes the use of AFR technology by the police. The second part focuses on the supervision mechanism proposed by the Home Office in the Biometrics Strategy. However, because the use of AFR technology is still controversial, this article will sort out the key issues of follow-up development through the opinions of the public and private sectors. The overview of the discussion of AFR technology used by police agencies would be helpful for further policy formulation.

II. Overview of the strategy of AFR technology used by the UK police

According to the Home Office's Biometrics Strategy, the AFR technology will be used in law enforcement, passports and immigration and national security to protect the public and make these public services more efficient[1]. Since 2017 the UK police have worked with tech companies in testing the AFR technology, at public events like Notting Hill Carnival or big football matches[2].

In practice, AFR technology is deployed with mobile or fixed camera systems. When a face image is captured through the camera, it is passed to the recognition software for identification in real time. Then, the AFR system will process if there is a 'match' and the alarm would solicit an operator's attention to verify the match and execute the appropriate action[3]. For example, South Wales Police have used AFR system to compare images of people in crowds attending events with pre-determined watch lists of suspected mobile phone thieves[4]. In the future, the police may also compare potential suspects against images from closed-circuit television cameras (CCTV) or mobile phone footage for evidential and investigatory purposes[5].

The AFR system may use as tools of crime prevention, more than as a form of crime detection[6]. However, the uses of AFR technology are seen as dangerous and intrusive by the UK public[7]. For one thing, it could cause serious harm to democracy and human rights if the police agency misuses AFR technology. For another, it could have a chilling effect on civil society and people may keep self-censoring lawful behavior under constant surveillance[8].

III. The supervision mechanism of AFR technology

To maintaining public trust, there must be a supervision mechanism to oversight the use of AFR technology in law enforcement. The UK Home Office indicates that the use of AFR technology is governed by a number of codes of practice including Police and Criminal Evidence Act 1984, Surveillance Camera Code of Practice and the Information Commissioner's Office (ICO)'s Code of Practice for surveillance cameras[9].

(I) Police and Criminal Evidence Act 1984

The Police and Criminal Evidence Act (PACE) 1984 lays down police powers to obtain and use biometric data, such as collecting DNA and fingerprints from people arrested for a recordable offence. The PACE allows law enforcement agencies proceeding identification to find out people related to crime for criminal and national security purposes. Therefore, for the investigation, detection and prevention tasks related to crime and terrorist activities, the police can collect the facial image of the suspect, which can also be interpreted as the scope of authorization of the PACE.

(II) Surveillance Camera Code of Practice

The use of CCTV in public places has interfered with the rights of the people, so the Protection of Freedoms Act 2012 requires the establishment of an independent Surveillance Camera Commissioner (SCC) for supervision. The Surveillance Camera Code of Practice proposed by the SCC sets out 12 principles for guiding the operation and use of surveillance camera systems. The 12 guiding principles are as follows[10]:

A. Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.
B. The use of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.
C. There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints.
D. There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.
E. Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them.
F. No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged.
G. Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.
H. Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.
I. Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.
J. There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published.
K. When the use of a surveillance camera system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value.
L. Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date.

(III) ICO's Code of Practice for surveillance cameras

It must need to pay attention to the personal data and privacy protection during the use of surveillance camera systems and AFR technology. The ICO issued its Code of Practice for surveillance cameras under the Data Protection Act 1998 to explain the legal requirements operators of surveillance cameras. The key points of ICO's Code of Practice for surveillance cameras are summarized as follows[11]:

A. The use time of the surveillance camera systems should be carefully evaluated and adjusted. It is recommended to regularly evaluate whether it is necessary and proportionate to continue using it.
B. A police force should ensure an effective administration of surveillance camera systems deciding who has responsibility for the control of personal information, what is to be recorded, how the information should be used and to whom it may be disclosed.
C. Recorded material should be stored in a safe way to ensure that personal information can be used effectively for its intended purpose. In addition, the information may be considered to be encrypted if necessary.
D. Disclosure of information from surveillance systems must be controlled and consistent with the purposes for which the system was established.
E. Individuals whose information is recoded have a right to be provided with that information or view that information. The ICO recommends that information must be provided promptly and within no longer than 40 calendar days of receiving a request.
F. The minimum and maximum retention periods of recoded material is not prescribed in the Data Protection Act 1998, but it should not be kept for longer than is necessary and should be the shortest period necessary to serve the purposes for which the system was established.

(IV) A new oversight and advisory board

In addition to the aforementioned regulations and guidance, the UK Home Office mentioned that it will work closely with related authorities, including ICO, SCC, Biometrics Commissioner (BC), and Forensic Science Regulator (FSR) to establish a new oversight and advisory board to coordinate consideration of law enforcement's use of facial images and facial recognition systems[12].

To sum up, it is estimated that the use of AFR technology by law enforcement has been abided by existing regulations and guidance. Firstly, surveillance camera systems must be used on the purposes for which the system was established. Secondly, clear responsibility and accountability mechanisms should be ensured. Thirdly, individuals whose information is recoded have the right to request access to relevant information. In the future, the new oversight and advisory board will be asked to consider issues relating to law enforcement's use of AFR technology with greater transparency.

IV. Follow-up key issues for the use of AFR technology

Regarding to the UK Home Office's Biometrics Strategy, members of independent agencies such as ICO, BC, SCC, as well as civil society, believe that there are still many deficiencies, the relevant discussions are summarized as follows:

(I) The necessity of using AFR technology

Elizabeth Denham, ICO Commissioner, called for looking at the use of AFR technology carefully, because AFR is an intrusive technology and can increase the risk of intruding into our privacy. Therefore, for the use of AFR technology to be legal, the UK police must

have clear evidence to demonstrate that the use of AFR technology in public space is effective in resolving the problem that it aims to address[13].

The Home Office has pledged to undertake Data Protection Impact Assessments (DPIAs) before introducing AFR technology, including the purpose and legal basis, the framework applies to the organization using the biometrics, the necessity and proportionality and so on.

(II)The limitations of using facial image data

The UK police can collect, process and use personal data based on the need for crime prevention, investigation and prosecution. In order to secure the use of biometric information, the BC was established under the Protection of Freedoms Act 2012. The mission of the BC is to regulate the use of biometric information, provide protection from disproportionate enforcement action, and limit the application of surveillance and counter-terrorism powers.

However, the BC's powers do not presently extend to other forms of biometric information other than DNA or fingerprints[14]. The BC has expressed concern that while the use of biometric data may well be in the public interest for law enforcement purposes and to support other government functions, the public benefit must be balanced against loss of privacy. Hence, legislation should be carried to decide that crucial question, instead of depending on the BC's case feedback[15].

Because biometric data is especially sensitive and most intrusive of individual privacy, it seems that a governance framework should be required and will make decisions of the use of facial images by the police.

(III) Database management and transparency

For the application of AFR technology, the scope of biometric database is a dispute issue in the UK. It is worth mentioning that the British people feel distrust of the criminal database held by the police. When someone is arrested and detained by the police, the police will take photos of the suspect's face. However, unlike fingerprints and DNA, even if the person is not sued, their facial images are not automatically deleted from the police biometric database[16].

South Wales Police have used AFR technology to compare facial images of people in crowds attending major public events with pre-determined watch lists of suspected mobile phone thieves in the AFR field test. Although the watch lists are created for time-limited and specific purposes, the inclusion of suspects who could possibly be innocent people still causes public panic.

Elizabeth Denham warned that there should be a transparency system about retaining facial images of those arrested but not charged for certain offences[17]. Therefore, in the future the UK Home Office may need to establish a transparent system of AFR biometric database and related supervision mechanism.

(IV) Accuracy and identification errors

In addition to worrying about infringing personal privacy, the low accuracy of AFR technology is another reason many people oppose the use of AFR technology by police agencies. Silkie Carlo, director of Big Brother Watch, said the police must immediately stop using the AFR technology and avoid mistaking thousands of innocent citizens as criminals; Paul Wiles, Biometrics Commissioner, also called for legislation to manage AFR technology because of its accuracy is too low and the use of AFR technology should be tested and passed external peer review[18].

In the Home Office's Biometric Strategy, the scientific quality standards for AFR technology will be established jointly with the FSR, an independent agency under the Home Office. In other words, the Home Office plans to extend the existing forensics science regime to regulate AFR technology.

Therefore, the FSR has worked with the SCC to develop standards relevant to digital forensics. The UK government has not yet seen specific standards for regulating the accuracy of AFR technology at the present stage.

V. Conclusion

From the discussion of the public and private sectors in the UK, we can summarize some rules for the use of AFR technology. Firstly, before the application of AFR technology, it is necessary to complete the pre-assessment to ensure the benefits to the whole society. Secondly, there is the possibility of identifying errors in AFR technology. Therefore, in order to maintain the confidence and trust of the people, the relevant scientific standards should be set up first to test the system accuracy. Thirdly, the AFR system should be regarded as an assisting tool for police enforcement in the initial stage. In other words, the information analyzed by the AFR system should still be judged by law enforcement officials, and the police officers should take the responsibilities.

In order to balance the protection of public interest and basic human rights, the use of biometric data in the AFR technology should be regulated by a special law other than the regulations of surveillance camera and data protection. The scope of the identification database is also a key point, and it may need legislators' approval to collect and store the facial image data of innocent people. Last but not least, the use of the AFR system should be transparent and the victims of human rights violations can seek appeal.

[1] UK Home Office, *Biometrics Strategy*, Jun. 28, 2018, https://www.gov.uk/government/publications/home-office-biometrics-strategy (last visited Aug. 09, 2018), at 7.

[2] Big Brother Watch, *FACE OFF CAMPAIGN: STOP THE MET POLICE USING AUTHORITARIAN FACIAL RECOGNITION CAMERAS*, https://bigbrotherwatch.org.uk/all-campaigns/face-off-campaign/ (last visited Aug. 16, 2018).

[3] Lucas Introna & David Wood, *Picturing algorithmic surveillance: the politics of facial recognition systems*, Surveillance & Society, 2(2/3), 177-198 (2004).

[4] Supra note 1, at 12.

[5] *Id*, at 25.

[6] Michael Bromby, *Computerised Facial Recognition Systems: The Surrounding Legal Problems* (Sep. 2006)(LL.M Dissertation Faculty of

Law University of Edinburgh), http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.197.7339&rep=rep1&type=pdf , at 3.
[7] Owen Bowcott, *Police face legal action over use of facial recognition cameras*, The Guardian, Jun. 14, 2018, https://www.theguardian.com/technology/2018/jun/14/police-face-legal-action-over-use-of-facial-recognition-cameras (last visited Aug. 09, 2018).
[8] Martha Spurrier, *Facial recognition is not just useless. In police hands, it is dangerous*, The Guardian, May 16, 2018, https://www.theguardian.com/commentisfree/2018/may/16/facial-recognition-useless-police-dangerous-met-inaccurate (last visited Aug. 17, 2018).
[9] Supra note 1, at 12.
[10] Surveillance Camera Commissioner, *Surveillance camera code of practice*, Oct. 28, 2014, https://www.gov.uk/government/publications/surveillance-camera-code-of-practice (last visited Aug. 17, 2018).
[11] UK Information Commissioner's Office, *In the picture: A data protection code of practice for surveillance cameras and personal information*, Jun. 09, 2017, https://ico.org.uk/for-organisations/guide-to-data-protection/encryption/scenarios/cctv/ (last visited Aug. 10, 2018).
[12] Supra note 1, at 13.
[13] Elizabeth Denham, *Blog: facial recognition technology and law enforcement*, Information Commissioner's Office, May 14, 2018, https://ico.org.uk/about-the-ico/news-and-events/blog-facial-recognition-technology-and-law-enforcement/ (last visited Aug. 14, 2018).
[14] Monique Mann & Marcus Smith, *Automated Facial Recognition Technology: Recent Developments and Approaches to Oversight*, Automated Facial Recognition Technology, 10(1), 140 (2017).
[15] Biometrics Commissioner, *Biometrics Commissioner's response to the Home Office Biometrics Strategy*, Jun. 28, 2018, https://www.gov.uk/government/news/biometrics-commissioners-response-to-the-home-office-biometrics-strategy (last visited Aug. 15, 2018).
[16] Supra note 2.
[17] Supra note 13.
[18] Jon Sharman, *Metropolitan Police's facial recognition technology 98% inaccurate, figures show*, INDEPENDENT, May 13, 2018, https://www.independent.co.uk/news/uk/home-news/met-police-facial-recognition-success-south-wales-trial-home-office-false-positive-a8345036.html (last visited Aug. 09, 2018).

Links

- Biometrics Strategy
- FACE OFF CAMPAIGN: STOP THE MET POLICE USING AUTHORITARIAN FACIAL RECOGNITION CAMERAS
- Police face legal action over use of facial recognition cameras
- Facial recognition is not just useless. In police hands, it is dangerous
- Surveillance camera code of practice
- In the picture: A data protection code of practice for surveillance cameras and personal information
- Blog: facial recognition technology and law enforcement
- Biometrics Commissioner's response to the Home Office Biometrics Strategy
- Metropolitan Police

Download

- Computerised Facial Recognition Systems: The Surrounding Legal Problems [7339&rep=rep1&type=pdf]

Wu, Tsai-Wei
Legal Researcher

Release : 2019/12

Tag

巨量資料 資訊安全