Case-based Analysis of Discrimination in Police Surveillance Scene Regarding Facial Recognition

Tingyao Chen*

Law School, the South China University of Technology, Guangzhou 510006, China

*13824450795@163.com

Abstract. The application of facial recognition technology in police surveillance scene is justified, but it will result in discrimination. In this paper, the first case of facial recognition in the world, R (Bridges) v Chief Constable of South Wales Police, is taken as the starting point, and the problems of algorithmic discrimination and indirect discrimination reflected in this case are discussed while analyzing the case, and the author will predict what kind of method the plaintiff may take in the appeal.

1. Context

Facial recognition technologies, or face id, are biometric systems that combine the advantages of the humans' amazing skill of perception with the benefits of immense processing power and memory capacity of computers [1]. In the case, plaintiff R (Bridges) accused South Wales Police (SWP) of improper use of automatic facial recognition technology (AFR), which automatically processes images containing faces to verification, identification or surveillance, and it mainly uses the biological information feature of the human face to distinguish individuals [2]. Verification is the process of verifying whether a person is a match with a specific individual stored in the system, and it is a one-to-one process in face information matching [3]. Identification can be divided into the closed-set identification and the open-set identification. The former is the information of the object to be identified which has been stored in the database and designated and it is only necessary to compare the individual face information with the information to be recognized; the latter can be understood simply as the recognizer does not know whether the face information to be recognized is already stored in the database [4]. Surveillance is usually a many-to-many process, in which the AFR collects facial information from a non-specific individual to compare it with non-specific individuals in the database who may be suspected of committing a crime, and the determination of the suspect standard will be determined by the recognizer according to the specific circumstances or regulations to set up different algorithms.

The monitoring process of SWP using AFR Locate for facial recognition belongs to a many-to-many process, and it is roughly divided into the following steps: First, to establish a facial information database or watch list to store the information of individuals with illegal records or criminal suspects; Second, the CCTV real-time monitoring function is used to capture suspects’ facial information in moving crowds, which is the main process of facial information collection. The system then extracts images from the video to determine whether it contains human faces and categorizes the images that contain different faces. The system then extracts facial features from the images, and the images will be compared with the individuals on the watch list. Finally, based on matching similarity SWP will determine whether the identified facial information is on the watch list. The construction of SWP’s facial
information database is based on the needs of previous police activities and investigation of specific cases, and the corresponding threshold is set for the system in each recognition to avoid the false-positive rate of the results. When the system has matched, both images are first reviewed by an AFR operator with the identity of a police officer, who confirms the match is accurate and then sends it to the intervention officers for review. SWP has developed the ‘traffic light’ system to help the examiner determine the urgency of the match, but not interfering with the examiner's opinion. AFR Locate will delete the face data if the result shows no match.

SWP consults the Surveillance Camera Commissioner on the use of Surveillance cameras and chooses the location of each AFR deployment based on the location of a particular crime and the need to maximize the collection of facial information. Despite this, many people who have their faces captured by AFR claim that they do not aware of this fact when AFR is used.

2. Facts
In this case, the plaintiff Mr. Bridges sued SWP because SWP was illegally using AFR, for the reason that the plaintiff’s facial information was captured by SWP respectively at Queen Street Cardiff on 21 December 2017 and in Defence Procurement, Research, Technology and Exportability Exhibition on 27 March 2018 without the plaintiff's consent, according to which the plaintiff argued that the defendant had violated Article 8 of the European Convention on Human Rights, the Data Protection Act 1998 (DPA 1998) and the Data Protection Act 2018 (DPA 2018), and the s149(1) of Equality Act 2010.

3. Issue
In response to Article 8 of the European Convention on Human Rights, the plaintiff found that the defendant had violated the Right to respect for private and family life by using AFR to collect information on human faces without his consent. In the case of the s4(4) DPA 1998 and s35 of DPA 2018, the plaintiff held that the defendant had failed to meet the requirements of the first Data Protection principle and had violated the obligation of assessment under the s64 DPA 2018. The plaintiff also claimed that the defendant failed to consider the possibility of a false positive result during the early evaluation phase of the adoption of the NeoFace system, which resulted in a violation of the "promotion of equal relations" requirement of the s149(1) Equality Act 2010. In this case, SWP recognized the plaintiff's status in the judicial review process and recognized his eligibility as a victim under section 7 of the Human Rights Act 1998, and relieved the plaintiff of the burden of proofing that the image of his face had been collected actually, for the court to pass judgment on the substantive issues involved in the case.

4. Analysis
In response to Article 8 of the European Convention on Human Rights, the court invokes R. Wood V. The commission of Police of the Metropolis and believes that the core values of Article 8 are "physical and psychological integrity" and "physical and social identity". It also supports the claim that the SWP's collection of facial information without the plaintiff's consent and plaintiff did not have any prior criminal record, violates Article 8, and constitutes an interference with individual autonomy. The use of AFR by the defendant without the plaintiff's consent falls within the scope of the right to privacy protected by this article, and the instantaneous and transient nature of the data processing does not affect the infringement judgment, because the fact that the AFR processes biological information is in itself a sufficient violation of Article 8 rights, and SWP's use of AFR is not a "predictable and unsurprising" simple photograph. The plaintiff claimed that the use of AFR Locate had to have a real legal basis, and the court reasoned that it was reasonable to place AFR Locate under the common law framework. The common law gives the police the power to police and punishes crime, including the power to make public the portraits of suspects and the power to use personal portraits to prevent crime. The AFR's access to information is not physically intrusive, and the police have the power to use personal portraits fairly obtained through AFR for crime prevention purposes, and there is no need to create new legal instruments for each new technology. Based on the determination of the common law hearing, the court
established three frameworks for the analysis of the legitimacy of the AFR, namely, the primary legislation, secondary legislative instruments, and SWP’s local policies. Based on the infringement, the court analyzed the justification of SWP’s use of AFR Locate and borrowed the four-part test from Bank Mellat v Her Majesty’s Treasury. Since a reasonable connection between the proportionality test and conduct and objectives can be demonstrated by police practice, the main consideration is whether the SWP’s conduct is less intrusive and whether it strikes a balance between individual rights and community interests. The court found that AFR was used for a specific time, place, and purpose, with limited coverage and obvious benefits from its use. Besides, the court denied the plaintiff’s claims that the use of AFR was not necessary, that it was not targeted in its application and that it did not improve the SWP’s ability to detect crimes, and therefore the court could consider that both of these criteria were met, namely that the violation of Article 8 rights by AFR was justified.

Secondly, in respect to the plaintiff’s claim that SWP did not fulfill its obligations as the data controller under DPA 1998 s.4(4), the court’s examination of whether SWP’s conduct was consistent with the first data protection principle was premised on an understanding of concepts such as "personal data". The court referred to the definition in Directive 95/46/EC and held that the definition should be defined in terms of both indirect identification and personalization. The problem in the indirect identification path is that if the information collected by AFR Locate does not conform to the definition of personal data, then the SWP will belong to personal data according to the matching result obtained by the information in the future. Drawing on the broad interpretation of indirect recognition given by CJEU in the Breyer v Bundesrepublik Deutschland, the court stated that all reasonable means used by the controller to identify an individual should be included in indirect recognition unless it falls within the scope of the risk of identification "appears in reality, to be significant". The second path to personal data is the individual, which is the ability to fully identify individuals in a crowd by analysing the facial information collected. The court decided that the individual path was more appropriate based on the AFR pattern and further considered whether SWP’s actions were consistent with the first data protection principle. In cases where both the plaintiff and the SWP agree that the facial information does not belong to sensitive information, the court only needs to examine whether the SWP’s behaviour complies with Schedule 2 and finds that Paragraph 6’s analysis of the data processing necessity is the focus of the review. The court uses the same reasoning as Article 8 to explain the legality of the SWP’s behavior, i.e., there is no violation of DPA 1998.

The plaintiff’s facial information was collected twice before DPA 2018 came into effect, but both parties argued that it is necessary for the court to review whether the defendant's use of AFR conforms to DPA 2018. The plaintiff claimed that the defendant had violated s. 35 (3) sensitive treatment relates to the interpretation of "biometric data". The court upheld the plaintiff’s claim that s. 35 (3) collection of "biometric data" covered both individuals on the watch list and the general public, and that the collection of "biometric data" by the public had to meet s.35 requirements. The court recognized both "the Processing is strictly necessary for the Law Enforcement purpose" and the Processing must meet at least one of the conditions in Schedule 8, but questioned the appropriateness of the "Policy on Sensitive Processing for Law Enforcement Purposes" formulated by the SWP and indicated a need for Information Commissioner guidance.

The plaintiffs also relied on DPA 2018 s.64 to assert that SWP had not conducted a Data Protection Impact Assessment before using AFR Locate, but SWP had provided a "Privacy Impact Assessment" of 12th February 2018 to demonstrate that it had fulfilled its assessment.

Obligations. The court found that the assessment issued by the SWP was clear, took into account the impact on the public’s right to privacy, identified the legal risks of AFR Locate’s use and the possibility of violation in practice, and was consistent with Article 8 of the European Convention on Human Rights.

The plaintiffs also argued that SWP’s use of facial recognition software, called NeoFace Watch, resulted in indirect discrimination based on the s149(1) Equality Act 2010 that did not take into account false positive results, i.e., AFR Locate has a higher error rate in identifying women and minorities. The court found that there was no evidence that the SWP had known or should have known in its earlier assessment that indirect discrimination would result and that it had not been established that the use of
AFR Locate would necessarily result in indirect discrimination. While the plaintiff’s expert witness, Dr. Anil Jain, cannot collect information from the AFR Locate database to determine whether the system may have caused indirect discrimination, it contends that SWP also cannot accurately analyse the information in the database, it is therefore argued that the SWP should not use AFR Locate where there is a risk of discrimination. As a representative of SWP, Dominic Edgell proposed that the high false-positive rate of women in the matching results was due to the system’s recognition of female facial features. The court held there is no conclusive evidence at this time that the AFR has an indirectly discriminatory effect, although whether the AFR Locate has an indirectly discriminatory effect at this time needs to be further determined. However, this does not mean that in the past the SWP failed to comply with its obligations under the s149 (1) Equality Act 2010, and the court dismissed the plaintiff’s claim.

5. Comments
The discrimination consequences of matching results seem to be a common feature of AFR Systems, which involves the discussion of algorithmic discrimination. AI Now’s 2019 Report introduces some cases of algorithmic discrimination [5]. David Heine Meier Hansson, a prominent software engineer, found that Apple Card gave him 20 times as much credit as his wife, and Janet Hill as the wife of Apple co-founder Steve Wozniak, has only a tenth of her husband’s credit limit. Although the design of the algorithm does not contain discriminatory factors at the code level, the data in the training set of the system are biased to different groups, such as race and age distribution, which leads to discriminatory results [6]. An article on the ICO blog analyses the gender bias involved in loan quotas, meaning that the algorithm, when applied to a loan assessment, builds a statistical model that requires a sample to be filled in to assess an individual's credit limit [7]. If the sample is male-dominated, the system will not be able to accurately judge the ability of women to repay loans, and then reduce the number of women's loans, which in the results show indirect discrimination against women. Technology companies have taken notice of algorithmic discrimination, but the protection of citizens' Anti-Discrimination Rights has given way to huge commercial interests. Google Chairman Eric Schmidt has said publicly that companies are aware of algorithmic discrimination and there is no need for too much public attention to algorithmic discrimination. Companies such as Amazon and Facebook have also spoken out against the regulation of facial recognition, arguing that it would affect the development of the industry, which actually to maintain the lucrative business of facial recognition. AFR’s algorithm plays an important role in the process of facial recognition, and the discrimination result caused by AFR error recognition belongs to the category of algorithmic discrimination in essence.

In the present case, the plaintiff claims that SWP constitutes indirect discrimination on the basis that SWP violated its evaluation obligation under the Equality Act 2010, and that non-discrimination has different sources in European Union Law. For example, Article 14 of the European Convention on Human Rights (ECHR) and Article 21 of Charter of Fundamental Rights of The European Union (The Charter) both stipulate non-discrimination. The Charter's anti-discrimination provisions are similar to ECHR, but broader and set out as a separate right, making its protection not subject to other provisions. There are also specific directives or ordinances regulating the situations of discrimination enumerated in the Charter, such as Gender Equality Directive (Recast, 2006/54/EC), Gender Equal Access Directive (2004/113/EC) and Racial Equality Directive (2000/43/EC) in the aspect of race and ethnicity. The definition of indirect discrimination in Racial Equality Directive (2000/43/EC) is that which shall be taken to occupy where a neutral vision, criterion or practice would put persons of a racial or ethnic origin at a particular advantage compared with other persons. Indirect discrimination is difficult to avoid in the statistical model built by the algorithm since the matching result is often affected by the number of images and the skin color of the people collected by AFR, since the accuracy of skin color recognition has large differences in different light conditions, and these differences are usually difficult to be improved through mathematical or technical methods. The AFR's black box structure makes it impossible to know the factors that influence the results of the specific processes of facial information collection, recognition, and matching. Therefore, even if AFR is found to have indirect discrimination
results, people can also sue AFR users who violate their fundamental rights under different regulations, and this situation cannot be effectively improved in a short period.

The admission of SWP in this case relieved the plaintiff of the burden of proof that his face information had actually been collected, but the court stated in its judgment that the plaintiff's substantive rights had not been violated. The plaintiff's allegation that the SWP's use of AFR Locate resulted in indirect discrimination was also denied by the court. It is worth noting that the plaintiff accused SWP of constituting indirect discrimination rather than direct discrimination. However, from the perspective of the probability of victory, once SWP constitutes direct discrimination, it must constitute a violation of the Equality Act. In other words, if SWP carries out direct discrimination, there is no room for defense in law, and SWP shall directly bear the illegal consequences. However, even if the SWP constitutes indirect discrimination, it does not necessarily have to bear responsibility, as for example, Directive 2000/43/EC provides that as long as the suspected act of indirect discrimination is objectively proved to have a legitimate aim and the manner of achieving that aim is appropriate and necessary, then the act does not amount to indirect discrimination. So when the plaintiff sued SWP for indirect discrimination, SWP could claim that the use of SWP was following the exception clause, which increased the burden of proof of the plaintiff. A reasonable explanation is that SWP's use of AFR Locate does not qualify as direct discrimination, so the plaintiff turns to indirect discrimination. According to the BBC, Lord Justice Singh granted the plaintiff's appeal in this case [8]. At the appeal stage, the author thinks that the plaintiff can continue to insist that SWP constitutes indirect discrimination but also needs strong evidence to show that SWP's indirect discrimination has had an adverse effect or absorb the victims who have suffered actual losses into the appeal procedure. Black, Asian, and minority ethnic (BAME) groups showed greater attention to the AFR's prior consent, meaning that Bame was more likely to suffer harm in the AFR's implementation scenario [9]. If Bridges can persuade the actual victims of indirect racial discrimination -- those who suffer inequality treatment because of AFR Locate's use and their race -- to join the appeal, SWP could be sued under Directive 2000/43/EC for violation of the s.2 (1) prohibition of indirect discrimination, increasing the probability of success while also reducing the risk of AFR Locate continuing to produce discriminatory results until the risk assessment is fully completed.

References

[1] Welinder, Yana. (2012) A face tells more than a thousand posts: Developing face recognition privacy in social networks. Harv. JL & Tech. 26: 165.
[2] Selvadurai, Niloufer. (2015) Not just a face in the crowd: addressing the intrusive potential of the online application of face recognition technologies. International Journal of Law and Information Technology 23.3: 187 - 218.
[3] Lucas D. Introna and Helen Nissenbaum, Centre for Catastrophe Preparedness and Response. (2020) Facial Recognition Technology: A Survey of Policy and Implementation Issues., 4 - 5.
[4] Ibid., 3.
[5] AI Now. (2019) AI NOW 2019 REPORT. https://ainowinstitute.org/AI_Now_2019_Report.pdf.
[6] Yavuz C. (2019) Machine Bias: Artificial Intelligence and Discrimination [J]. SSRN 3439702: 21 - 22.
[7] ICO. (2019) Human bias and discrimination in AI systems. https://ico.org.uk/about-the-ico/news-and-events/ai-blog-human-bias-and-discrimination-in-ai-systems.
[8] Nick Dermody. (2019) Facial recognition technology: Ed Bridges appeals human rights ruling. https://www.bbc.com/news/uk-wales-50495575.
[9] Ada Lovelace Institute, (2019) Beyond face value: public attitudes to facial recognition technology., 8 - 18.