

# Analysis of the Legal Restrictions of Facial Recognition—— From the Perspective of Wechat's Use of Facial Recognition Technology to Identify Criminals

Jingyi Chen \*

Chinese University of Hong Kong, Hong Kong, China

\* Corresponding Author Email: jingyichen99@outlook.com

**Abstract.** The facial information collected by facial recognition technology belongs to the biometric information that should be protected by the relevant sensitive information laws or regulations. Because of the importance and uniqueness of facial information, we need to use facial information legally so as not to violate people's right to privacy and equality. In this article, we explore the norms for the use of facial recognition technology by private organisations, such as WeChat, which uses facial recognition technology to track down criminals who sexually assault young people. Specifically, we discuss several aspects, including the photos collected by private organizations that fall under the jurisdiction of the law, the consent or permission of the relevant public sectors before the private organization uses facial recognition technology, the consent of users before their photos are used, and the compliance to avoid violating the rights to equality and privacy.

**Keywords:** Facial Recognition Technology, Rights of Equality, Rights of Privacy.

## 1. Introduction

Facial recognition technology is becoming increasingly popular, not only in public safety but also in the private sector. The technology is used in a wide range of applications, including time and attendance and unlocking mobile phones. However, the widespread use of facial recognition technology has created a problem of infringement. According to existing rulings in different jurisdictions, many people claim that information collected by facial recognition technology violates their right to privacy and equality. Facial recognition technology captures people's biometric information, which is unique and personal to each individual. If the collection, storage and deletion of facial recognition technology are not regulated, people's biometric information is likely to be stolen or leaked. As this type of information is irreplaceable, there will be no other remedies if this information is maliciously altered and used [1]. As a result, private lawsuits brought by individuals over the use of the technology have contributed to the development of facial recognition laws.

WeChat has recently started using facial recognition technology to track down criminals who have committed sexual offences against minors. As facial recognition technology is controversial, the legitimacy of this practice should be examined more closely. This paper will focus on four different aspects. First, whether the photos collected by WeChat's facial recognition technology fall within the scope of biometric information. Second, what are the requirements for WeChat, as a private organisation, to collect sensitive information from users using facial recognition technology? Third, what are the legal restrictions on WeChat's use of facial recognition technology? Finally, what are the legal compliance requirements for private organisations such as WeChat?

## 2. Whether the Facial Recognition Information Falls Under the Jurisdiction of the Law

### 2.1. Facial Recognition Technology Needs to Comply With Bio-identifiable Information Specifications

Facial recognition technology involves obtaining the geometric information of people's faces through biological measurements, and the system matches the person's facial information with

photographs stored in the system to determine whether they are the same person. In *Rivera v. Google* [2], Rivera alleged that after taking a photograph of herself and uploading it to the Google Droid, Google scanned her facial features and developed a unique facial template without her consent, in violation of the Biometric Information Privacy Act. Google argued that the Privacy Act governs the process of facial recognition to scan facial geometry information, whereas Google was simply capturing facial information from photos submitted by people. Therefore, this practice was not subject to the Privacy Act. In addition, the "Bio-metric Information Privacy Act" defines biometric information as the scanning of retina, iris, fingerprints, voiceprints, hands or faces. In addition to specifying biometric information, the Act includes a list of non-biometric information such as written signatures, images and demographic data [3]. So if you simply match a photo to the information on another photo, the Biometric Information Protection Act does not apply. However, I disagree with the opinion of Google. As technology advances, artificial facial recognition technology may now get bio-metric information not only from faces but also from photographs. The information carrier is not used to determine whether this conduct should be regulated, but rather the content of information that the user can acquire is the determinable factor. As long as the user acquires biometric information, the Personal Information Protection Law should regulate this conduct. Furthermore, even if the information collected from the photo is not bio-metric information, it still belongs to personally sensitive information. The data received from the photo should be regarded as personal private data with personal characteristics. As a result, it must be regulated by laws and cannot be abused by all organizations, especially private organizations.

## **2.2. Whether WeChat's Facial Recognition Technology falls under the Jurisdiction of the Law**

Facial recognition technology is a neutral technology and is not always illegal. To determine whether this technology is illegal, it must be weighed against the area and method of use. If the facial recognition is based on a photograph taken during public surveillance, and the goal is to protect public safety, this conduct is legal and can be considered a robot cop doing his duty. However, if the facial recognition information comes from private domains, you should be aware of whether it is breaking the rules and invading your privacy. If WeChat's facial recognition technology collects images that users share in Moments to identify and monitor criminal suspects, this practice should be regulated by the Personal Information Protection Law. This is because according to the People's Republic of China's "Personal Information Protection Law", people's facial geometric features are bio-identifiable information, and the images collected by WeChat are bio-identifiable information.

Even if WeChat's acquisition of private images falls under the scope of the Personal Information Protection Law, it is a lawful act if it complies with the Personal Information Protection Law and other related laws. Specifically, the consent of the parties must be obtained before using their facial information. WeChat may violate people's privacy and personal information protection rights if it obtains private images without users' prior consent. This is because the behaviour of collecting private photos is protected by law, even for public security purposes, which means that excessive intrusion into the private sphere is not allowed. In the *Matter of Residence in Oakland* case [4], it can be demonstrated that even when the government arrests criminals, it cannot force them to use their biometric information, such as fingerprints and faces, to unlock electronic devices. This means that the government's use of a search warrant to collect the public's biometric information must be justified; otherwise it violates the public's right to privacy. In other words, privacy should be protected. We also need to clarify the scope of private areas so that we can avoid violating the right to private areas. From this case, we can conclude that the private area refers to the area that meets the objective recognition of society and the subjective recognition of people. Therefore, due to the fact that WeChat moments are private property, if WeChat wants to access images shared by users, it should notify them and obtain their permission. Otherwise, even if the goal of using facial recognition technology is to track down criminals, WeChat will be considered to be violating people's right to privacy.

### **3. Prerequisites for Facial Recognition Technology to Obtain the Public's Sensitive Information**

#### **3.1. Conditions for Public Sectors to Obtain Facial Recognition Information**

Because the purpose of the facial recognition information collected by the public sector is in the public interest or for public safety, the public sector may use this technology to carry out its functions in a discretionary manner. *Beach v. OKLAHOMA DEPT. OF PUBLIC SAFETY* case [5], the local safety department required the plaintiff to submit images to update his driver's license so that the department could use facial recognition technology to detect illegal activity on the road. The plaintiff claimed that the local security department's actions violated her religious beliefs. However, the court ultimately sided with the defendant, reasoning that in this case the defendant collected the plaintiff's photographs for public safety purposes and there was no other improper use of the photographs. More importantly, the defendant was acting within the scope of his powers to carry out public functions. At the same time, in the case of *R (Bridges) v CCSWP and SSHH* [6], the South Wales Police indicated that they had used artificial facial recognition technology to locate some targets that were already on the police's terrorist watch list. It is the duty of the police or other appropriate government agencies to apprehend criminal suspects, and they have the authority to do so in public. Road surveillance is also in accordance with the applicable regulations, and its methods of pursuing suspects are within the scope of its powers. At the same time, Article 34 of the "Law on the Protection of Personal Information" states that government agencies have the inherent power to do so if the purpose of the processing of personal information by them is for public security or public interest. At the same time, Article 34 of the "Personal Information Protection Law" stipulates that the conduct of government agencies that use facial recognition data within the scope of their authority to track down criminal suspects does not endanger people's privacy or other rights.

#### **3.2. Conditions for Private Organizations to Obtain Facial Recognition Information**

However, the majority of facial recognition technologies are invented and used by private companies, not government agencies. As for the private organisations, their use of facial recognition technology to detect and monitor criminal suspects requires government authorisation or consent. Since private companies do not have the authority to search for criminals, they cannot catch or search for criminals on their own. Meanwhile, it is difficult for the police to find criminal suspects who are anonymous or disguised, and the existing system used by local public security departments makes it impossible to find suspects without criminal records, so the police need the support of public organisations to use facial recognition technology. As a result, we can see that the police often cooperate with private companies that use facial recognition technology to track down criminal suspects. However, even if a private organisation is authorised to use this technology with the consent of the relevant public authorities, it must ensure that it does not misuse public power to violate the public's right to privacy.

In addition, the private organisation needs to be supervised by the public sector. If WeChat needs to use facial recognition technology to find criminal suspects who have committed sexual crimes with children, the police need to cooperate with WeChat and share the suspect's photo to match the suspect's photo with the huge number of photos in the system. The criminal suspect's information is classified as confidential police information, so it must be protected. However, private organisations such as WeChat can not only know the relevant information, but also influence the outcome of the match through the technical control system. In addition, private companies such as WeChat possess critical biometric information collected from users, and once the information is leaked, irreversible damage may occur. Therefore, private organisations need to be supervised and managed using information from the police and users.

Specifically, Article 53 of the "Personal Information Protection Law" stipulates that in order to protect personal information, a special agency or designated representative must be established in China, and the name of the relevant agency or representative, as well as contact information, must be

submitted to the relevant department. This rule aims to make it easier for relevant authorities to manage the collection of facial information by private companies. This is because as early as 2007, a company sold consumers' fingerprints and property information to avoid bankruptcy, resulting in the leakage of the public's bio-identifiable information [7]. Therefore, the law will strictly regulate this behaviour because personal biometric information is unique and important. It is difficult to seek redress when biometric information is altered or leaked. In particular, WeChat, as a private company responsible for collecting important and private personal information, should be strictly regulated. Although the purpose of collecting bio-identifiable information is for public safety, Wechat must still report to relevant authorities and accept their supervision to ensure that its behaviour does not violate relevant laws or regulations on personal information protection.

## **4. Legal Restrictions on the Use of Face Recognition Technology**

### **4.1. Clarify the Legitimacy of the Purpose and the Use of Facial Recognition Technology**

In addition to regulating the subject that uses facial recognition technology, it is important to regulate the process of using facial recognition through legislation. To begin with, Article 6 of the "Personal Information Protection Law" should clarify the purpose of using artificial facial recognition technology. In addition, the use and purpose of facial recognition technology must be in accordance with legal, just and necessary standards. In the *Rosenbach v. Six Flags Entertainment* case [8], the plaintiff, who had purchased amusement park tickets for his child online, was forced by the defendant to provide his son's personal information. At the same time, the plaintiff's son is required to complete the personal information registration process in order to visit the amusement park. In this case, the plaintiff alleged that the defendant had not informed him, in writing or otherwise, of the specific purpose of collecting his son's fingerprints, thereby violating his son's right to privacy and autonomy over personal information. Where parties are required to provide biometric information, they must be informed of the aim and purpose of the action and be given the opportunity to accept or refuse the decision to provide the information. In the case of *R (Bridges) v CCSWP* [9], the police inform the public when they collect bio-identifiable information from people under surveillance and ensure that the public has the right to withdraw. First, to ensure that the public understands the purpose, method and conduct of biometric data collection and can make informed choices. Secondly, to ensure that all members of the public have access to the information and that there is no information gap in order to establish the legitimacy of the activity. In addition, to ensure the public's right of withdrawal, the public has the opportunity to opt out of providing biometric information.

At the same time, in China's first facial recognition case [10], the plaintiff, Guo Bing, held the Wildlife World annual pass. Wildlife World advised the plaintiff to scan his fingerprints upon entering the zoo. On the same day, the defendant sent a message to the plaintiff requesting the plaintiff to activate the annual card on the use of facial information. Otherwise, the plaintiff would not be able to enter the zoo. In this case, the court found that the defendant's initial collection of fingerprint information was for the purpose of informing the parties and obtaining their consent, and that the information was collected in accordance with the Consumer Protection Act's criteria of lawfulness, fairness and necessity. However, the court found that the collection of facial recognition data was unlawful. This is because the plaintiff was only asked to provide fingerprint information when applying for the annual pass, and later the zoo proposed to provide facial recognition information more than the principle of necessity; meanwhile, the plaintiff's original fingerprint information would not affect his admission to the zoo, so the acquisition of the plaintiff's facial information is illegal. In addition, the defendant acquired the plaintiff's facial information during the information-gathering process without the plaintiff's consent. The court held that the defendant collected facial information without the plaintiff's permission or consent, which violated the party's right to consent and the protection of personal information. Although the Personal Information Protection Law had not been enacted at the time of this case's verdict, the judge still found that the act violated the party's right to privacy and right to know the purpose of the use of their private information under the

Consumer Protection Law. In conclusion, from three cases, Wechat should inform users of the purpose and use of facial recognition technology, and the purpose of using this technology should be consistent with lawfulness, fairness and necessity.

#### **4.2. Clarify the Legitimacy of the Source of Information Obtained by Facial Recognition Technology**

When facial recognition technology is used to obtain bio-identifiable information, individuals must be informed of the purpose and intent of the data collection and must consent to participate in the activity. Three factors need to be considered when obtaining consent from users.

First, the purpose of using artificial facial recognition technology should be examined. If the public sector is using facial recognition technology within the limits of its powers for public interest or public security purposes, it only needs to notify the parties before using the technology. However, if it is for any other reason, the parties' consent is required.

Second, consider the source of the information collected by facial recognition technology. If the information comes from the public domain, it is considered public information and does not require the consent of the party concerned; however, if the information comes from the private domain, the consent of the party concerned must be obtained before using the information.

Finally, it is important to remember that if the information collected is sensitive, the parties' consent must be obtained. For example, if WeChat wants to obtain private images of the public in order to track criminal suspects, it must obtain the parties' consent. Specifically, WeChat, as a private entity, uses facial recognition technology to assist the government in carrying out public law enforcement functions. From this perspective, the goal of Wechat's use of facial recognition technology is to ensure public safety. At this level, I think Wechat only needs to notify users rather than obtain their consent; however, at the second level, it is necessary to consider the source of the information collected by WeChat. The information is derived from private photos, and the photos published on WeChat at the moment are not public. This is because photos in Wechat's Moment can be shown to certain users' friends. Although Weibo pictures are shown to the public, if you want to use those photos, you need to get the permission of the owners [11]. On the other hand, compared to Weibo, Wechat photos are only displayed among specific friends. Therefore, WeChat is one of the private areas, which means that Wechat needs to get permission before using users' photos.

It is important to clarify the source of facial recognition data. Two types of information sources need to be distinguished: those in the public domain and those in the private domain. When facial information is used in the public security domain, private privacy must be weighed against the goals of protecting public safety, and there may be times when private privacy needs to be fairly restricted. However, when facial recognition technology is used in the private sector, strong privacy safeguards must be implemented to prevent invasions of personal privacy [12]. This is because we need to protect social welfare in the public sphere, so we may sacrifice some of people's private rights. But we need to protect private welfare in a private area in order to prevent the public authority from violating the right to privacy. Although the source of the information received by WeChat comes from a private area, the parties who share their facial information must give their prior consent.

Specifically, in the case of *R (Bridges) v CCSWP and SSHH*, the police used public surveillance cameras to gather information, which was also in accordance with the relevant laws and regulations. This behaviour did not invade people's privacy. Moreover, this behaviour took place on a street during the operation of facial recognition technology. The police used the camera on the police car to collect information, and the police car was covered with signs. From the facts, we can see that this behaviour does not belong to secretly taking pictures of the public. In fact, this behaviour is the legal duty of the police. However, the information sources used by WeChat belong to the private sphere. Therefore, in order to obtain photos uploaded by the public through technical means, WeChat must obtain the public's consent in advance. Otherwise, this behaviour constitutes a violation of the privacy rights of the parties concerned, resulting in the illegality of the source of the obtained photos.

Most importantly, the information obtained through WeChat is sensitive information. According to the PRC's "Personal Information Protection Law", the processing of sensitive personal information requires individual consent. Therefore, whether it is a state agency or an individual agency, both require public consent if they want to obtain people's sensitive information. Therefore, WeChat must obtain the parties' consent in advance before carrying out this activity, otherwise it will constitute a violation of the parties' information protection rights.

However, due to gaps in the current legal system, private organisations such as WeChat use broad privacy clauses to circumvent legal restrictions. For example, most private organisations now believe that if parties do not seek the opt-out method, they have obtained users' consent. But does agreeing to such standard terms constitute consent? Is it effective? In addition, when private organisations collect or store parties' information, they promise to protect users' privacy and not to share private information with others. However, if the information relates to public safety, these organisations will cooperate with the police to review the information. So how do you define the boundaries between protecting public safety and protecting privacy?

Regarding obtaining the public's consent, if the private organization decides to update the privacy policy and the user's consent privacy policy, will this behaviour be regarded as the user's consent? I think this behaviour cannot be regarded as consent using users' images, although Article 10 of the "Personal Information Protection Law" stipulates that the subject of personal information taking the initiative to declare, taking the initiative to check, taking the initiative to click "agree" and other methods constitute express consent. However, as the subject of personal information collection, the privacy clauses they have entered into are standard clauses, and the parties negotiate and modify them. It is not essentially the voluntary consent of the public [13]. In particular, if the parties do not agree on Wechat's privacy clauses, they will not be able to use WeChat's software. Meanwhile, the WeChat platform has a high degree of customer dependence, so the parties will not easily give up using WeChat, which means that they are forced to agree to the privacy terms. Customers are not willing to give up WeChat because the cost of switching to other platforms will be very high, which means that the public will not only be unable to contact friends on WeChat, but also unable to use financial services and other services. Therefore, it is suspected that if consent is obtained by updating the privacy policy, the party will be forced to provide personal information. The "Personal Information Protection Law" stipulates that it is illegal to force personal information subjects to provide personal information. Therefore, WeChat should separate the consent to use users' private photos from the use of Wechat functions.

## **5. Compliance Requirements of Private Organizations Including Wechat**

### **5.1. The Necessity of Compliance Caused by Private Privacy Litigation Rights**

The use of facial information by private organisations requires compliance with the law, which primarily includes compliance with privacy and equality rights. This is because the law gives the private party the right to sue the party using facial recognition technology directly. This means that even if the party does not have actual damages, the party can file a lawsuit and obtain compensation and redress from the private organisation involved in the improper use of the party's biometric information [14]. In the Facebook case [15], Facebook collected, used and stored the parties' bio-identifiable information without the parties' written consent, which violated Article 15(b) [16]. It also failed to delete the related information within a reasonable time, which violated Article 15(a) [17]. Therefore, the court upheld the plaintiff's claim. At the same time, in *Rosenbach v. Six Flags Entertainment* [18], the court held that as long as the violation of Article 15 of the Act constitutes an infringement of the party's right to biometric information, there is no need to prove the consequence of additional damage. The court held that this was the purpose of the legislation to mitigate the results of the plaintiff's proof of damages, which can ensure that parties can be protected before the biometric information is leaked or stolen.

Second, by imposing significant potential liabilities on the private organisation that violates the law, it can encourage parties to exercise self-discipline through compliance behaviour. Although this places more responsibility on the private organisation, it is reasonable. Through compliance, the private organisation can ensure that the collection, storage and deletion of personal biometric information are in accordance with the law. Although private organisations have to bear more costs when collecting personal information, they can ensure the protection of personal information. Unlike other information, which can be changed if it is leaked, facial information is biometric information, which is unique, and once it is leaked, there is no remedy. Therefore, the costs borne by private organisations are insignificant compared to the substantial and irreversible damage caused by the leakage of biometric information. And imposing more responsibilities and obligations on information collectors through legislation can promote the development of social privacy protection.

## **5.2. The Need for Compliance Arising from the Protection of the Right to Equality**

In addition to complying with the Privacy Act, private organisations must also comply with the equality provisions of the Bill of Rights when using facial recognition technology. In the case of *R (Bridges) v. CCSWP and SSHH* [19], the plaintiff claimed that the defendant's use of facial recognition technology violated the PSED, the Bill of Rights, because the technology used by the defendant discriminated on the basis of race and gender. Although the court ultimately did not uphold the plaintiff's claim, it found that there was no evidence that the technology produced discriminatory results. However, it is difficult for technology to be 100% accurate. If more and more false positives occur, it will inevitably encourage the development of legislation against such behaviour. Therefore, private information collectors need to implement the compliance of the right to equality with artificial facial recognition technology [20]. Although the public hopes that private organisations can make the technology transparent and provide evidence that it does not discriminate against people of different races and genders. But it is difficult to achieve this goal because facial recognition technology is protected as a trade secret. It is therefore difficult to promote the transparency of technology from private organisations in a short period of time. Promoting self-censorship within private organisations can not only ensure that the public's right to equality is not violated, but also protect the trade secrets of private organisations. However, simple internal compliance is not enough and needs to be monitored by a neutral third party to ensure that it does not lead to racial and gender discrimination. Therefore, it is necessary to review the facial recognition technology and evaluate the potential matches generated by the software before using this technology; otherwise the next step cannot be continued. The development of the technology will promote the legal requirements to disclose facial recognition technology, but facial recognition technology as a trade secret, once disclosed, will seriously affect the development of the company. Therefore, the company needs to conduct internal compliance governance and cooperate with professional organisations, the third party or the government to make the final confirmation after collecting facial information, to avoid the occurrence of incidents that violate people's right to equality.

In addition, both the police and private organisations will have a bias against the people they are tracking. They will have a preference in providing information about the targets of surveillance. The police or private organisations can search for anyone they are interested in, which violates the right to equality. Therefore, it is necessary to limit the discretion of the police and regulate the search power of private organisations. In particular, since WeChat helps the police track down criminal suspects, the relevant departments should regulate the behaviour of WeChat that abuses its power. The public power of the police also needs to be regulated, as the police prefer to provide information on criminal suspects to Wechat.

## **6. Conclusion**

The legality review of Wechat's behaviour in tracking criminal suspects through facial recognition is mainly based on the protection of personal information and the right to equality. With the

promulgation of the Personal Information Protection Law, more and more attention is being paid to the protection of personal information. As a result, private organisations must comply with more standards when collecting sensitive information. Second, as facial recognition technology is essentially an artificial intelligence technology, it is inevitable that the system will have deviations, and the deviations may lead to racial and gender discrimination. Therefore, private organisations need to conduct internal compliance reviews to ensure the legality of their actions.

## References

- [1] Andrejevic M, Selwyn N. Facial recognition technology in schools: critical questions and concerns[J]. Routledge, 2020, 45(2):115-128.
- [2] Bennett, K. A. Whether Bennett face recognition technology can be used in a new way of anti-terrorism —— constitutionality research based on face recognition monitoring system [J]. National Journal of Justice Technology, 2001,3:151.
- [3] Ferguson, Andrew Three. Facial recognition and the Fourth Amendment [J]. Minnesota Revision, 2020,105:1105.
- [4] McClellan E. Facial Recognition Technology: Balancing the Benefits and Concerns[J]. J. Bus. & Tech. L., 2019, 15: 363.
- [5] Zhou torrent, Zhang Ye. Research progress in face recognition Theory [J]. Journal of Computer-Aided Design and Graphing, 1999,11 (2): 180-184.