Introduction

On 9 Apr. 2021, the Hangzhou Intermediate People's Court, the court of second instance, issued its judgment in Guo Bing v. Hangzhou Safari Park Co., Ltd., [(2020) Zhe 01 Min Zhong No. 10940], the first civil dispute case concerning facial recognition in China, arousing attention on the topic of personal biometric information security in all walks of life.

Summary of the case

Facts: The defendant Hangzhou Safari Park ("the Park") sold annual passes to tourists and indicated that tourists could enter the Park with their annual passes and fingerprints. The plaintiff Guo Bing ("Guo") and his wife purchased the annual pass from the Park in April 2019, and the Park collected their fingerprints and profile photos.

In July 2019, the Park introduced facial recognition technology replacing the original fingerprint recognition system. Later, the Park sent text messages to Guo twice, informing him of the replacement of the annual card identification system and asking Guo to activate the facial recognition system, otherwise he would not be able to enter the park normally. Guo refused to accept the activation on the grounds that facial information is highly sensitive and personal privacy, and asked the Park to return the annual pass fee. After the two sides failed to negotiate, Guo sued the Park to the People's Court of Fuyang District in Hangzhou on October 28, 2019.

Arguments:

1. Confirm that the contents of the notices and SMS notices concerning fingerprint identification and face recognition in the store of the Park are invalid.
2. The Park shall compensate for the annual card fee and the transportation fee and other expenses incurred to solve the dispute.
3. The Park deletes all personal information submitted by Guo Bing.

Judgement:

First instance: 1. Wildlife World compensates Guo Bing for loss of contract interests and transportation expenses totaling RMB 1,038; 2. Wildlife World deleted Guo Bing's facial features, including photos, submitted when he applied for the annual fingerprint card; 3. Guo Bing's other claims shall be rejected. Both Guo and Wildlife World have appealed.[1]

Second instance: 1. Items 1 and 2 of the judgment of first instance shall be upheld; 2. Annulling the third judgment of the first instance; 3. Wildlife World deleted the fingerprint identification information submitted by Guo Bing when he applied for the annual fingerprint card; 4. Guo Bing's other claims shall be rejected.[2]

---

[1] *Guo Bing v. Hangzhou Safari Park Ltd* [2019] Zhe 0111 Min Chu No. 6971

[2] *Guo Bing v. Hangzhou Safari Park Ltd* [2020] Zhe 01 Min Zhong No. 10940

Analysis

The court did not support argument 1, stating that Chinese law does not prohibit the collection and use of personal information in the consumer domain. Instead, it emphasizes the principle of "legal, legitimate, and necessary" collection with the consent of the parties involved. The Park's use of fingerprint identification and other technologies to verify the identity of annual card users and improve park entry efficiency was deemed to meet these principles.

Regarding Argument 2, the court supported Guo's claim. The Park unilaterally change the way to enter the park constitutes a breach of contract, should compensate Guo Bing contract loss.

Regarding Argument 3, the court supported Guo's claim. While Guo had agreed to fingerprint recognition when purchasing the annual pass, the collection of facial recognition information went beyond the principle of necessity. The park did not inform Guo about the facial recognition purpose, violating the principle of justification. As a result, the first- instance court ruled that the park should delete Guo's photo but determined that there was no need to delete his fingerprint.

The second-instance court upheld the first-instance court's view on the principles of "lawful, justified, and necessary" collection of personal information. It emphasized that

> *"biometric information, being sensitive and reflecting physiological and behavioral characteristics, carries significant personal attributes. Leaking or illegal use of such information could lead to discrimination or endanger personal and property safety, necessitating cautious treatment and protection."*[3]

The second-instance court agreed with the first-instance court's ruling, ordering the park to delete Guo's photo. Additionally, since the park had ceased using fingerprint recognition, there was no justification for retaining Guo's fingerprint. Consequently, the second-instance court overturned the first-instance ruling related to fingerprints and directed the park to delete Guo's fingerprint as well.

Commentary

1. **The importance of principles of notification and voluntary choice：** according to the judgment in argument 1, the primary criteria for judging whether personal information has been infringed are the principles of notification and voluntary choice. This means that users have the right to be informed when their personal information is collected by enterprises, and they can decide whether to allow their personal information to be collected. The Data Security Management Measures (Draft for Comments) released in May 2019 fully clarified this principle. [4]
2. **The difference between the first and second cases**: it is mainly reflected in the importance of personal

[3] The supreme people's court, 'A typical case of the People's Court serving and safeguarding the integrated development of the Yangtze River Delta' (*The Supreme People's Court of the People's Republic of China*, 2 November 2021) <https://www.court.gov.cn/zixun-xiangqing-329801.html> accessed 27 April 2023

[4] Data Security Law of the People's Republic of China 2021

information protection. The judgment of the first instance is mainly based on the Contract Law.[5] Judging whether personal information should be deleted is based on the criterion of breach of contract and based on the result. The perspective is relatively narrow. The judgment of the second instance reflects the high attention to the protection of personal information, effectively preventing the possibility of personal information leakage and illegal use.

The subsequent Civil Code,[6] Personal Information Protection Law[7] and relevant judicial interpretations are very consistent with the comprehensive protection of personal information embodied in the second instance judgment of this case. According to the provisions of A.14 to A.16 of the Personal Information Protection Law and A.4 of the Provisions of the Supreme People's Court on several issues relating to the application of law in civil cases involving the use of face recognition technology to process personal information[8], personal information processing personnel shall not force or disguised force natural persons to agree to process their face information. Therefore, the judgment view of the court of second instance is very forward-looking, but also has a strong guiding significance for the trial of subsequent cases.

3. Consider the legal background to the case and revisit it under the new law

This case took place before the Civil Code was enacted, so the General Provisions of the Civil Law[9], Contract Law, Tort Liability Law[10], and Protection of the Rights and Interests of Consumers[11] were applicable. While these regulations may appear strict, they are actually weak when it comes to consumer information protection. The Tort Liability Law, for instance, follows a "wrongdoer-damage" attribution principle stated in Article 6, requiring Guo to prove that his personal information was infringed upon by the park and caused actual loss in order for his claim to be recognized by the court. Thus, if the Park argues that face recognition is meant to enhance efficiency and optimize the visitor experience, the act of collecting consumers' facial information may not qualify as a "fault act" under the Tort Liability Law, making it difficult for the court to rule in favor of Guo's infringement claim.

However, the personal information protection challenge in Guo Bing's case is likely to be resolved with the implementation of the Civil Code[12] on January 1, 2021. Article 1,034 of the Civil Code explicitly states that personal information is protected by law, defining it to include biometric information such as fingerprints and facial data. It further specifies that processing personal information without the consent of the individual constitutes an infringement.

If we reassess the case in light of the new civil code:

---

[5] Contract Law of the People's Republic of China 1999

[6] Civil Code of the People's Republic of China 2020

[7] Personal Information Protection Law of the People's Republic of China 2021

[8] Provisions of the Supreme People's Court on several issues concerning the application of law to the trial of Civil Cases concerning the use of facial recognition technology to process personal information 2021

[9] General Principles of the Civil Law of the People's Republic of China 1986

[10] Tort Law of the People's Republic of China 2010

[11] Law of the People's Republic of China on the Protection of Consumers' Rights and Interests 1993

[12] Civil Code of the People's Republic of China 2021

Firstly, personal information is no longer within the vague realm of rights protection but becomes a legally recognized right of personality.

Secondly, it establishes the exercise of the right to claim personal information protection, eliminating the need to prove fault on the part of the infringer and abandoning the traditional "fault behavior-damage" model. It also does not require the infringer's actions to result in actual loss for the victim.

In this legal context, even if the Park argues that face recognition aims to improve efficiency and enhance the visitor experience and there is no unlawful use of Guo Bing and his wife's personal information, the court may still find the Park liable for infringing on their personal information rights based on the relevant provisions of the Civil Code and the specific circumstances. The court would require the park to cease the infringement and eliminate the associated risks.

4. Implications

For businesses, the use of information data tools enhances customer selection and operational efficiency, but it also entails increased responsibilities. Enterprises must strictly adhere to legal provisions, ensure voluntary information collection, rational use, and robust prevention of data breaches. Failure to do so may result in infringement claims and potential financial compensation and damage to their reputation.

For individuals, personal information is closely tied to various aspects of life and property. Therefore, it is crucial to prioritize personal information protection. When providing personal information, individuals should exercise caution and carefully consider the implications. In the event of personal information infringement, it is important to utilize legal measures to actively safeguard one's legitimate rights and interests.

Conclusion

This case represents the first face recognition dispute in the context of the digital economy. It safeguards the legitimate rights and interests of consumers regarding their facial identification information and other identifying data while standardizing the collection of biometric information. The judgment takes into account the dual needs of promoting digital industry development and protecting personal information, offering guidance for similar cases in the future. It aligns with the increasing trend of personal information protection under the Civil Code.