Lifting the Veil of Mystery in Facial Recognition: Privacy Protection from Private Entities' Misuse of Information in China

Xingjie Huang
School of Law, City University of Hong Kong, Hong Kong, China
xingjie_huang@126.com

Abstract: In the past few years, improvements in facial recognition technology have caused a rapid increase in the collection of facial recognition information in the private sector. In China, data subjects' facial recognition information could be easily collected with or without their knowledge as they enter into some public business premises such as hotels, banks, and other physical public places. As public spaces extend to digital public spaces, the collection of facial recognition may happen online. For example, platform providers extract and collect facial recognition information from uploading photos publicly available online, with or without data subjects' consent. Privacy concerns unavoidably come with the illegal collection of facial recognition information. Personal Information Protection Law (PIPL) regards facial recognition information as sensitive information and sets up rules to protect data subjects' facial recognition information from illegal collection by private entities in physical public places. However, the law has not yet fully developed to protect this information effectively, and more privacy issues happen in China. Later, several regulations and judicial interpretations are established to address the issues, especially issues in physical public places. This essay endeavours to examine data subjects' informational privacy rights regarding facial recognition information and whether existing Chinese regulatory mechanisms are effective enough to protect their rights to facial recognition information from the misuse of information by private entities in public spaces. After discussing the nature of facial recognition information, this article points out that issues in the illegal collection, process, and use of facial recognition information by private entities potentially intersect with both the protection of personal information and informational privacy protection. Data subjects' informational privacy rights regarding facial recognition information deserve protection. Next, it conducts a comparative analysis to compare rules regulating the misuse of facial recognition information in the private sector among the EU, the US, and China. It finds that different jurisdictions have different focal points, which lead to different protection patterns. The EU protects data subjects' informational privacy rights regarding facial recognition information as fundamental rights, and the US prioritizes the free flow of information, while China focuses on the specific activities of data processors. Finally, it proposes that the Chinese pattern could be improved to protect data subjects' privacy rights to facial recognition information comprehensively, such as by flexible application of the informed consent principle.
Keywords: Facial Recognition Information; Informational Privacy Rights; The Misuse of Facial Recognition Information in the Private Sector; Physical Public Places and Digital Public Spaces; Chinese Regulatory Mechanisms

1. INTRODUCTION

In the past few years, facial recognition techno logy has become increasingly popular in China. Both public authorities and private entities show their preference for applying facial recognition technology. This article mainly focuses on the collection of facial recognition information in the private sector. Private companies have viewed facial recognition technology as a means of safeguarding their users' sensitive information, employing multi-factor authentication (MFA) as a security measure against identity theft (Corbit, 2022). For example, facial recognition cameras are commonly installed at the entrances of malls, hotels, animal parks, cultural institutions, various public spaces, and private residences for verifying identity. However, the improper collection of facial recognition information by private entities in public spaces may result in privacy issues. Consider the case of Xu v. Pintai Company (Pintai). In this case, the plaintiff Xu visited the sales office of the defendant Pintai. Pintai installed CCTV cameras with the facial recognition function in the sales office and used them to capture photographs of visitors. Pintai notified that the facial recognition system was applied on sites for internal security purposes, but it failed to explicitly state that the system was also used to collect and store consumers' facial information for identification. Xu's face was captured during the visit, and the screenshots were saved. Accidentally, Xu found that the facial recognition system was subsequently used to identify her, and her facial recognition information was retained, not deleted upon expiration. Consequently, an issue arose between Xu and Pintai regarding the collection of facial recognition information. The aforementioned case highlights the challenges faced by data subjects in obtaining accurate information regarding the precise purpose of facial recognition information collection and providing timely consent. If a significant number of data subjects' facial images are collected illegally by private entities, either online or offline, or if a substantial amount of discrete facial recognition information is amassed across various databases in an unlawful way, data subjects will lose control over their fundamental biometric information, the facial recognition information. Correspondingly, their informational privacy interests might be compromised. The improper collection in the private sector poses a direct threat to the data subject's facial recognition information. This article aims to argue whether Chinese regulations on the collection of facial recognition information in public spaces in the private sector are effective enough to protect data subjects' privacy rights to facial recognition information. It first figures out the

nature of facial recognition information and the data subject's informational privacy rights to facial recognition information. Next, it conducts a comparative analysis of regulations on the collection of facial recognition information in public spaces by private entities in the EU, the US, and China. This document highlights the varying perspectives on informational privacy among the three jurisdictions, leading to distinct focal points of protection for each jurisdiction's regulatory framework. The regulations are a reflection of the unique regulatory essences of each jurisdiction. Finally, it argues that current regulations in China could be improved to protect data subjects' privacy rights to facial recognition information by taking some measures like filling the loopholes in regulating the collection in digital public spaces and a flexible application of the informed consent principle.

2. IS FACIAL RECOGNITION INFORMATION PRIVATE

2.1. From Facial Recognition Technology to Facial Recognition Information

Facial recognition technology is a biometric recognition technology based on human facial features information. It consists of a camera and an algorithm. Once the camera captures faces, the algorithm recognizes those faces by using biometric technology (McClellan, 2019). According to the different matching magnitudes, the purpose of facial recognition technology is classified into three different types, namely face authentication (1:1 mode), face recognition (1: N mode), and face retrieval (M: N mode). Facial recognition technology tracks facial features in photos or videos through camera capturing, automatically detects and compares facial patterns, and then recognizes the detected faces. The working process of facial recognition technology could be divided into five steps: image acquisition, face detection, feature extraction, database comparison, and identity recognition (Kaur et al., 2020). It converts photos into machine-readable digital information. It digitizes, deconstructs, and stores facial image information (Carrero, 2017), and compares them with the existing facial templates stored in the database (Mann & Smith, 2017). Facial recognition information is an important type of biometric information contained in the dataset of data subjects (Berle & Berle, 2020), which consists of two parts, one is the original facial images, and the other is the facial digital information generated by the technology. It has both the physiological characteristic and the behavioral characteristic (Carrero,

2017), which means that facial recognition information could be either static or dynamic. The former is about the shape and composition of the body, and the latter is related to individual behaviours.

2.2. The Nature of Facial Recognition Information

As mentioned above, facial recognition information is a type of biometric information, which is highly exclusive. The nature of facial recognition information is regulated in China, the EU, and the US. Both China and the EU consider facial recognition information to be a particularly sensitive or special type of personal information. China defines the meaning of sensitive personal information and lists several examples of sensitive personal information, among which examples are not exhaustive. According to Article 28 of the Personal Information Protection Law (PIPL), "sensitive personal information" refers to personal information that, if leaked or misused, could result in the infringement of an individual's dignity or cause harm to their safety or property, such as biometric information. Instead of providing a detailed explanation of the significance of special personal data, the EU categorizes them in an exhaustive manner. Article 9 of the General Data Protection Regulation (GDPR) specifically addresses the processing of "special categories of personal data," and biometric data falls under this category. In contrast to China and the European Union, there are no explicit regulations that explicitly define the special or sensitive nature of facial recognition information. However, certain states have enacted biometric information protection laws to safeguard biometric information, including facial recognition information, which acknowledges its unique nature. For instance, the Biometric Information Privacy Act (BIPA) in Illinois is a specific law that provides protection for biometric information. It recognizes facial recognition information as biometric information. The nature of facial recognition information is inherently sensitive and special. A significant factor contributing to its sensitivity and specialty is its direct connection to embodied personal information, such as biometric information, as opposed to indexical personal information such as home addresses. This suggests that facial recognition information primarily pertains to an individual's control over the disposition of their own biometric information, facial images (Alterman, 2003). Another significant factor is its less intrusiveness. Facial recognition information is a less intrusive biometric information compared to others like fingerprints and irises. It can be collected remotely and seamlessly, even without physical contact with the data subject. When an individual enters public spaces, the facial

image is readily visible to everyone, unless the individual wears a mask in physical public places or the photo is mosaic online (in digital public spaces). Consequently, the collection of facial recognition information can be conducted improperly and secretly, even without the data subject's knowledge or consent. This raises privacy concerns and necessitates its protection as a sensitive and special type of information (Chan, 2021).

2.3. Data Subject's Informational Privacy Right Regarding Facial Recognition Information

There is ongoing debate regarding the legal status of concerns pertaining to the illegal collection of facial recognition information in China. Some Chinese scholars contend that issues related to the illegal collection of facial recognition information in public spaces should not be considered privacy concerns. From their perspective, facial information is readily accessible unless an individual resides in a secluded location, and it remains unchanged unless an individual undergoes cosmetic surgery to alter their appearance. Consequently, it is impossible to prevent others from gaining knowledge of an individual's facial features within society. Furthermore, individuals lack privacy interests in their facial images since they are publicly available. Additionally, they argue that facial recognition is essential for identifying specific individuals in daily social interactions, and communication between individuals also necessitates facial expressions. Consequently, they classify concerns about the illegal collection of facial recognition information in public spaces as personal information protection issues, rather than privacy concerns. The argument above appears somewhat unbalanced. The right to privacy could be categorized into two distinct types: informational privacy rights and physical/locational privacy rights. Informational privacy encompasses personal information that is inherently private in nature. It is crucial to acknowledge that the scope of personal information protection extends beyond informational privacy alone. While discussing the right to privacy, informational privacy is merely one aspect of this broader concept. From the negative perspective of rights, the right to informational privacy can be seen as a protective barrier that allows individuals to decide who has access to their personal information. On the other hand, from the positive perspective, it also encompasses the concept of control rights, granting individuals the legitimate authority to control their personal information (Moore, 2015). This article suggests that issues about the unlawful collection of facial recognition information may potentially intersect with both the protection of personal information and informational privacy protection. The public-

private dichotomy is not the determinant of informational privacy in public spaces. In fact, informational privacy in public spaces is a bundle of dynamic and variable information relationships. The level of publicly accessible in public spaces and the form of personal information determine the existence of informational privacy in public spaces. Even when people are present in public spaces, they retain the right to be respected for their personal information. What they seek to preserve as private could be protected if there is a reasonable expectation of privacy. In public spaces with limited public access, such as private restrooms, individuals tend to have higher expectations for privacy; conversely, in public spaces that are readily accessible, such as streets, individuals may have lower expectations. The fact that an individual's facial image is easily reachable or accessible in public spaces does not automatically mean that there are no barriers against others and individuals forfeit their rights to control access to their facial recognition information. Accessibility does not diminish their entitlement to informational privacy and their ability to determine who has permission to interact with their information.

The form of personal information also influences individuals' informational privacy. In issues about the illegal collection of facial recognition information, what matters is not a facial image per se, but the systematic gathering and analysis of facial recognition information collected in public spaces. While a single facial image may not reveal substantial information about data subjects, the cumulative process of such information collection can lead to the compilation of comprehensive dossiers on individuals (Dul, 2022). Individuals might not have the expectation of privacy to the exposure of their facial images in public spaces, but they generally do not expect that more detailed information will be inferred from their facial images. This potentially reshapes their original expectations of privacy. In other words, the collection of facial recognition information in public spaces that facilitates the transmission and inference of facial recognition information is more likely to alter data subjects' expectations of privacy.

The illegal collection of facial recognition information, particularly through high-tech tools equipped with artificial intelligence (AI) capabilities, has the potential to elevate privacy concerns for data subjects (Madiega & Mildebrath, 2021). Consequently, data subjects shall have the informational privacy rights to safeguard their facial recognition information from unlawful collection in public spaces by private entities.

3. COMPARATIVE ANALYSIS—PRIVACY PROTECTION FROM THE MISUSE OF FACIAL RECOGNITION INFORMATION IN THE PRIVATE SECTOR

3.1. Right-Centered Protection in the EU

In the EU, a culture of privacy has been established, centered around the concept of "rights talk" (Schwartz & Peifer, 2017). A framework that prioritizes the protection of the data subject's personal information has been implemented. This framework ensures that individuals possess fundamental rights, the right to privacy, and empowers them to maintain control over their information. Following the principle of "rights talk", the EU adopts strict measures to protect the data subject's right to privacy, limiting the collection of facial recognition information in private sectors. The EU adopts a comprehensive legislative protection model for face information protection. Initially, it took the biological information protection in the General Data Protection Regulation (hereinafter referred to as "GDPR") as the core and recently extended to the artificial intelligence algorithm applied to facial recognition information. GDPR is the benchmark for the protection of personal information. It empowers data subjects' rights to protect their personal information. It differentiates the requirements for the process between general personal information and special categories of personal information. In Article 6, one of the requirements for the lawfulness of processing personal information is that data subjects shall give consent. Article 9 requires that the process of biometric information to uniquely identify a natural person shall be prohibited unless data subjects give explicit consent and other reasonable exceptions such as processing for substantial public interests (Regulation, 2016). The principle of consent applies to the process of all kinds of personal information, but it is stricter in special categories of personal information, such as biometric information. In addition, another important act, the Regulation of The European Parliament And of The Council Laying Down Harmonised Rules On Artificial Intelligence And Amending Certain Union Legislative Acts (Artificial Intelligence Act, 2021 version) differentiates several scenarios for the application of facial recognition. For example, the real-time collection or post-collection of facial recognition information by private sectors in public places is forbidden, unless it satisfies the strict requirements listed in the Act (EUROPEIA, 2021). Later, the Artificial Intelligence Act was amended, and the final version was approved by the European Council on 21st May 2024. The latest version of regulating the collection of facial recognition information became

somewhat stricter. According to this version, facial recognition technology is regarded as a high-risk AI system. Article 5 regulates "the placing on the market, the putting into service for this specific purpose, or the use of AI systems that create or expand facial recognition databases through the untargeted scraping of facial images from the internet or CCTV footage" shall be prohibited. This mentions the protection of data subjects' facial recognition information in digital public spaces (i.e., the Internet). It tends to even ban the collection of facial recognition information by private entities in physical public places for the purpose of identifying individuals. The new version reflects the EU's value of "right-centered" protection. The activities of collecting facial recognition information by data processors would be forbidden if their actions pose harm to the data subjects' interests. The EU's attempt to regulate the collection of facial recognition information is in favor of the protection of the data subject's privacy rights.

Table 1: The EU's laws are as Follows

General Data Protection Regulation (GDPR)	**Explicit consent**
Artificial Intelligence Act (AI Act)	A high-risk AI system

3.2. Market-Directed Regulations in the US

In contrast, the US's approach differs significantly from the EU's. In the US, data subjects are protected as "privacy consumers" (Schwartz & Peifer, 2017). Specifically, individuals are viewed as market participants engaged in market activities. Within the US's market-oriented narrative, the person is portrayed as a trader, dealing with their personal data as a commodity. The primary protection for personal information centers on facilitating the free flow of information rather than safeguarding the data subject's rights to privacy. Drawing from the concept of "marketplace discourse", the US's legal framework initially permits the unrestricted flow of information and only restricts the collection, process, and use of personal data when specific laws mandate it.

3.2.1. State Regulations

The California Consumer Privacy Act (CCPA) is a pivotal legislation that safeguards consumers' privacy. Although it was subsequently amended to the California Privacy Rights Act (CPRA), both two versions did not make any special provisions for biometric information. However, they do establish an opt-out regime that protects consumers' privacy rights. This opt-out rule permits users to decline cookies or reset them in the default browser setting where cookies are typically accepted and personal

information is collected. This aligns with the principle of the free flow of information in the US. Under section 1798.120(a) of the CCPA, businesses are mandated to inform consumers that their collected information may be sold and provide an option for consumers to opt out of the sale of their personal information. It underscores the paramount importance of obtaining the consent of the consumer prior to engaging in any business activity involving the sale of their personal information to third parties. Additionally, the CPRA restricts the collection of personal information, requiring private sectors to inform the purposes, categories, and duration of retention before the collection of personal information. Furthermore, the collection of consumers' personal information shall adhere to the principles of necessity and proportionality. The Biometric Information Privacy Act (BIPA) is the pioneering legislation at the state level that safeguards personal biometric information. In comparison to the BIPA, the CCPA and the CPRA offer relatively more permissive regulations on the collection of personal biometric information. Notably, these regulations do not establish distinct regulations for the collection of general personal information and biometric information. While the BIPA places greater emphasis on protecting biological information than the flow of information, the act recognizes biometric information as sensitive personal data that holds significant value in the US market. Consequently, stricter regulations are mandated to govern the collection of biometric information. Under the BIPA, private sectors are prohibited from collecting biometric information from individuals without prior notice and obtaining written consent. In addition, a significant contribution of this act is that it grants the data subject a private right of action. If the data subject's privacy rights are violated by the private sector under the provisions of the BIPA, they have the right to seek legal recourse in a state circuit court or add it as a supplementary claim in a federal district court against the offending private sector. The right of legal action serves as a powerful incentive for data subjects who have experienced privacy infringements to confront technology companies that collect their facial recognition information without their explicit consent. Class-action lawsuits have also been filed in response to these privacy violations. For example, in the case of Thornley v. Clearview AI, Inc., several victims collectively filed a lawsuit against Clearview AI for the collection and extraction of facial recognition information conducted without informed consent. Clearview AI, a prominent technology company, operates a facial search engine that indexes publicly accessible images of individuals online (Dul, 2022). The company develops facial recognition software that leverages the vast

amount of data available on the Internet to extract facial images from social media platforms. From each extracted image, the software collects the biometric facial scan along with related metadata, including timestamps and locations. Notably, Clearview AI failed to inform data subjects about the collection of facial recognition information or obtain their consent. Consequently, the court ruled that Clearview AI's actions constituted a statutory violation of the Biometric Information Privacy Act (BIPA). Another example is the class-action lawsuit Boone, et al. v. Snap Inc. In this legal proceeding, Snap Inc. faced allegations of violating the BIPA. The plaintiff asserted that the privacy policy of Snap failed to explicitly state the collection of users' facial information. Furthermore, the company was accused of scanning users' faces using filters and special effects lenses without obtaining the users' written authorization. Ultimately, the case was settled out of court, with the company agreeing to pay a $35 million settlement.

3.2.2. Federal Regulations

Currently, there are no federal laws that protect data subjects' facial recognition information. The Commercial Facial Recognition Privacy Act was introduced by Senator Roy Blunt on March 14, 2019, and has been passed twice by the US Congress. This act mandates that the collection of facial recognition information for commercial purposes is not allowed unless it obtains affirmative consent from data subjects (Blunt & Schatz, 2019). The term "affirmative consent" herein means that data subjects voluntarily and explicitly agree to the collection of facial recognition information. While there is no specific requirement for the form of consent, either verbal or written consent is acceptable. On the other hand, this act requires data controllers and processors to provide informative details about the collection of facial recognition information, including the purposes of collection, the length of data retention, and the practices of processors and controllers. Both the EU and the US emphasize the importance of clear notification and the data subject's consent, although informed consent is emphasized in different ways. While the GDPR does not specifically mention "opt-in", it mandates that data processors shall obtain the data subject's clear, positive, and informed consent before collecting data. This requirement, along with the criteria for valid consent, implies that opt-in consent is necessary before any data processing can take place in the EU. Unlike the EU, the US adopts the opt-out regime. It doesn't particularly stress the limitation on the collection of facial recognition information by private entities in physical public places. No

matter from the federal level or the state level, the US provides a guideline for data processors to collect personal information lawfully in the market. The primary objective of the regulations in the US is not to safeguard the data subject's informational privacy interests but rather to facilitate the unhindered flow of personal information.

Table 2: The US's laws are as Follows

State regulations	Biometric Information Privacy Act (BIPA), Illinois	Notice and consent in writing; A private right of action
	California Consumer Privacy Act (CCPA) & California Privacy Rights Act (CPRA)	Inform and consent
Federal regulations	Commercial Facial Recognition Privacy Act of 2019	Affirmative consent

3.3. Chinese Pattern

3.3.1. Personal Information Protection Law and the First Case of Facial Recognition

Initially, China fostered the development of facial recognition technology, and there were no strict regulations governing the collection of facial recognition data in private sectors. Article 26 of the PIPL mentions the requirement of the collection of facial recognition information in physical public places, stressing that the installment of facial recognition technology shall be with obvious signals, and its purpose shall be only for maintaining public safety, except with separate consent. Article 29 requires that the separate consent of the data subject is the basic requirement before processing sensitive personal information. Adhering to the opt-out rule setting in Article 26 of the PIPL, Article 21 of the Regulation on the Administration of Network Data Security (Draft for Comments) (2021) also emphasizes the separate consent of data subjects for the processing of biometric information. Actually the rules are either ambiguous or not very binding. Data processors may exploit vulnerabilities in regulations to engage in unlawful facial recognition information collection. Take the example of the first case of facial recognition—the case of Guo v. Hangzhou Wildlife Park. The plaintiff, Guo, purchased an annual family pass for entry to the defendant, Wildlife Park, and he provided personal information including their fingerprints and facial images recorded as required by Wildlife Park. During the execution of the service contract, Wildlife Park changed the entry method unilaterally without notifying Guo. Facial recognition has become the only entry

method. Guo argued that facial recognition information was highly sensitive to personal privacy and disagreed with its use. Negotiations between the two parties were unsuccessful, and Guo sued the court. This case went through the first and second trials. Due to the lack of clear and specific regulations on the collection of facial recognition information, the court finally turned to one of the general personal information protection principles, the principle of purpose limitation to address this issue. It stated that the activities of Wildlife Park disobeyed the principle of purpose limitation, which expanded the scope of the contract and went beyond the purpose of prior collection. Guo's facial recognition information was deleted by Wildlife Park in the end. This case indicates that the data subjects started to raise their awareness of protecting their facial recognition information. The court adheres to fundamental principles governing the collection, processing, and utilization of personal information to safeguard facial recognition information subjects from unlawful activities.

3.3.2. From the Permissive Regulation to the Restricted Regulation

Unlike the above rules, the national standard, Information Security Technology--Facial Recognition Information Security Requirement is a separate guidance for facial recognition, although it only serves as a recommended national standard without binding force. This standard tried to limit the activities of data processors. It states before collecting personal biometric data, individuals shall be informed separately about the purpose, method, and extent of the collection and use of such data, including storage duration and other regulations. Explicit consent is required before collecting personal biometric information. Since the first case involving facial recognition information, concerns regarding the unlawful collection of such data have been consistently raised in practice. To fill the gap in the existing law and regulation, as well as to address ongoing issues, the Provisions of the Supreme People's Court on Several Issues concerning the Application of Law in the Trial of Civil Cases Relating to the Processing of Personal Information by Using Facial Recognition Technology (the judicial interpretation) was established. The judicial interpretation clarifies eight types of misuse of facial recognition technology, one of which is the improper collection of facial recognition information in certain public places such as hotels, shopping centers, banks, stations, airports, stadiums, entertainment places, and so on. It points out that an individual who conducts the misuse of facial recognition information shall bear civil liability for infringing on the personality rights of the data subject. The judicial interpretation limits the collection of facial recognition information

by private entities in physical public places. For example, Article 10 regulates that where the property service provider or other building manager uses facial recognition as the only method to verify facial recognition for owners or property users to enter and exit the property service area, and dissenting owners or property users request other reasonable methods of verification to be provided, the people's court shall uphold such requests by the owners or property users who disagree with such request the provision of other reasonable methods of verification. This judicial interpretation could be considered as an indication of the tendency to restrict the collection of facial recognition information by private entities. Recently, the Provisions on Security Management of the Application of Facial Recognition Technology (for Trial Implementation) has been open to the public for comments. This trial version specifically restricts the collection of facial recognition information in physical public spaces based on the level of public accessibility of those spaces. Specifically, it further differentiates different scenarios of the collection of facial recognition information by private sectors in physical public places. It proposed to prohibit the installation of facial recognition devices with the function of image collection and identification in public places with a relatively private nature, like public bathrooms and public restrooms that may infringe on the privacy of others. Also, it requires that public business premises such as hotels, banks, stations, and so on shall not coerce data subjects to accept identification by collecting facial recognition information to promote service quality. Furthermore, regarding the use of remote and non-inductive facial recognition technology in general public places and public business premises, it limits the use of the technology unless admitted by data subjects to maintain national security and public safety and protect the life, health, and property safety of people in emergencies, without differentiating the law enforcement purpose and the private purpose. Furthermore, Article 14 of the trial version specifically prohibits communities and property management sites from collecting facial recognition information as the sole method of verifying an individual's identity for entry and exit purposes. This is an enhanced version of the judicial interpretation, which aims to mitigate the risk of similar issues to the first case of facial recognition information. It is also a rule with Chinese characteristics because of the community culture. The communities are allowed to set up the access control system for security purposes, but the system shall not be limited to the facial recognition system. With more detailed and restrictive implementing rules, this trial version appears to effectively safeguard data subjects' privacy rights regarding facial

recognition information. This is in line with the goal of combating the unlawful collection of facial recognition information. From PIPL to the trial version of the security management regulation, it is apparent that the Chinese pattern has changed from permissive regulation to restrictive regulation. With the advent of facial recognition technology in China, there was a notable absence of regulatory oversight governing the collection of facial recognition information in the private sector. A permissive regulatory framework was enacted to facilitate the advancement of facial recognition technology. Not only there are a few articles in PIPL regulating facial recognition, but even the articles regulating the collection of facial recognition information are too ambiguous to protect the data subject's facial recognition information effectively. Subsequently, as concerns regarding the unauthorized collection of facial recognition information in private sectors emerged, Chinese lawmakers recognized the imperative to enact stringent and comprehensive regulations governing the collection of facial recognition information by private entities. National standards, judicial interpretations, and several trial versions of regulations are released one after another. In principle, private entities are still permitted to collect facial recognition information in physical public spaces, albeit with more stringent regulations. For instance, the collected facial recognition information alone should not be the sole criterion for identifying individuals and granting access to certain physical public spaces. If data processors disobey the rules, they shall bear civil liabilities for their illegal collection. These regulations restrict the collection of facial recognition information by private entities and enhance the protection of data subjects' privacy rights regarding facial recognition information. They may contribute to reducing the number of privacy concerns related to the unauthorized collection of facial recognition information in public spaces.

Table 3(a): The Chinese laws are as Follows

Personal Information Protection Law (PIPL)	**Separate Consent**
The Regulation on the Administration of Network Data Security (Draft for Comments) (2021) Information Security Technology--Facial Recognition Information Security Requirement Provisions of the Supreme People's Court on Several Issues concerning the Application of Law in the Trial of Civil Cases Relating to the Processing of Personal Information by Using Facial Recognition Technology (the judicial interpretation)	Separate consent Provide alternative methods for data subjects to choose from Eight types of misuse of facial recognition technology; Civil liability; Not the only way to verify face recognition for owners or property users to enter and exit the property service area

Table 3(b): The Chinese laws are as Follows

Personal Information Protection Law (PIPL)	Separate Consent
The Provisions on Security Management of the Application of Facial Recognition Technology (for Trial Implementation)	Differentiates different scenarios of the collection of facial recognition information by private sectors in physical public places

3.4. Chinese Focal Point Leads to its Unique Protection Pattern

The primary focus of facial recognition information protection systems in China, the EU, and the US differ significantly. The EU directly safeguards facial recognition information by granting specific rights to data subjects and considers data subjects' privacy rights as a fundamental right. In contrast, although Chinese regulations also grant data subjects several rights to protect personal information, they primarily focus on safeguarding individuals' facial recognition information by regulating the activities of data processors. The US, on the other hand, prioritizes the core principles of information freedom in protecting facial recognition information. A notable distinction between Chinese regulations and those of the EU lies in the former's permissive stance towards private sector collection of facial recognition information in public spaces. In contrast, the EU generally restricts such collection to specific scenarios. The affirmative statement of the Chinese regulatory mechanism clarifies that Chinese regulations do not explicitly prohibit private entities from collecting facial recognition information in physical public spaces. The statement of Chinese rules is more affirmative, adopting the phrase "yes and requirement". In other words, most rules are written in an affirmative form, not forbidding the collection of facial recognition in public spaces but allowing data controllers/processors to collect facial recognition information with the condition of some limitations. One of the typical examples is Article 26 of PIPL. It permits the collection of facial recognition information in physical public places by private entities and establishes the requirements for the collection only for the purpose of maintaining public security, in a positive and affirmative statement. It appears that the affirmative statement offers greater space for data processors to justify the legality of their activities. In contrast, in the EU laws, the statement pertains to "no but exception," indicating that the collection of facial recognition information is prohibited in principle, except in cases where it meets specific criteria. For example, the collection of biometric information, such as facial recognition information, shall be

prohibited in principle, except for several scenarios listed in Article 9 of GDPR. This statement indicates that the EU remains cautious about the collection of facial recognition information in public spaces by private entities. Another difference between China and the US is the different methods of filing class action. Unlike the BIPA, which grants individuals the right of action against the data processors, in China, it is the people's procuratorate, the consumer organization designated by law, or the organization specified by the national cyberspace administration that may bring a class action against data processors for data subjects suffering from unlawful processing of personal information. For example, in the model case of procuratorial public interest litigation for personal information protection, Procuratorial Authorities of Huzhou City, Zhejiang Province v. Zhejiang G Tourism Development Co., Ltd. (G Company), G Company established a facial recognition system. The Huzhou Procuratorate stated that the company violated the law by not fulfilling its obligation to notify tourists when collecting their facial information with the system. The company forced ticket-buying tourists to register their facial information and use it to enter the scenic spot. The reason why the procuratorate intervened in the case is that the company's activities compromised the personal information of tourists and harmed the public interest. In China, the interests of the collective data subjects' facial recognition information are considered the public interest and are protected by administrative authorities, not individuals. Conversely, the US considers interests in individuals' facial recognition information as consumers' private interests, not the public interest. The US laws provide individuals with a private right of action to safeguard their own facial recognition information. Furthermore, in comparison to the protection patterns established in the EU and the US, the application of Chinese protection regulations appears to be confined to the collection of facial recognition data in physical public spaces. While the EU and the US have not explicitly mentioned the collection of facial recognition information in digital public spaces, their protection frameworks are capable of encompassing the scope of such collection in both physical and digital public spaces. Either the right-centered approach or the market-directed approach is sufficiently broad to safeguard the privacy rights of data subjects regarding facial recognition information, regardless of the location where such collection occurs. This is because these approaches prioritize the interests of informational privacy or the value of personal information circulation, rather than focusing on the specific activities of data processors. Regardless of the venue of the collection, the interests of informational privacy and the value of personal

information circulation warrant protection and balance. In contrast, Chinese regulations primarily focus on the activities of data processors in physical public spaces, overlooking privacy concerns in digital public spaces. In conclusion, the Chinese pattern adheres to the EU's unified legislation framework, establishing general law with specific implementing rules. It adopts an opt-out regime similar to the US, while its essence is distinct from that of the EU and the US. Notably, it neither emphasizes the sacred nature of the data subject's right to privacy nor the value of the free flow of personal information. Instead, it focuses on regulating the activities of data processors rather than establishing a framework for the protection of data subjects' rights to facial recognition information. Based on the logic of the Chinese pattern, as long as the activities of data processors are well-regulated, data subjects' privacy rights to facial recognition information will be effectively protected. However, as mentioned above, this protection method is limited. The effectiveness of the current Chinese mechanism in safeguarding data subjects' privacy rights to facial recognition information remains a subject of debate.

4. TO WHAT EXTENT COULD THE CHINESE PROTECTION PATTERN BE IMPROVED

4.1. Filling the Loopholes in Regulating the Misuse of Facial Recognition Information in Digital Public Spaces by Private Entities

4.1.1. The Potential Judicial Response to Privacy Issues in Digital Public Spaces

Current regulations primarily focus on the collection of facial recognition information in physical public spaces by private entities. However, there appears to be a lack of regulation on the collection, process and use of facial recognition information in digital public spaces. If cases involving the misuse of facial recognition information in digital public spaces are filed in China, how can the courts safeguard the informational privacy interests of data subjects? Prior to analyzing how China can address privacy concerns pertaining to the collection of facial recognition information in digital public spaces, this article will provide an illustrative example of Clearview AI to elucidate the nature of such issues. As previously mentioned, Clearview AI operates a facial search engine that indexes publicly accessible images of individuals online (Dul, 2022). Utilizing its proprietary algorithm, it extracts facial images from social media platforms that are accessible to the public. The extracted facial

information is subsequently stored within its database. Issues happen between Clearview AI and data subjects whose facial images are extracted. Unlike traditional privacy issues, these concerns transpire on online platforms, which constitute digital public spaces. The advancement of facial recognition technology has significantly expanded the scope of facial recognition information collection, encompassing both physical public spaces and digital public spaces. Currently, there are no specific regulations directly addressing the collection of facial recognition information in digital public spaces. If these issues are brought to court, general principles would be the primary approach to resolving them. One important principle is the informed consent. As mandated by law, the process of facial recognition information collection shall adhere to the requirement of informed consent from the data subject. PIPL stresses that separate consent must be obtained from individuals before processing sensitive personal information. Informed consent represents the exercise of an individual's right to self-determination over personal information. It stipulates that the collection of personal information is prohibited unless the data subject's consent is explicitly granted. Without the authorization and consent of the data subject, the data processors' activities on personal information are deemed to have no corresponding legal basis, and they are consequently held accountable for any legal consequences. The collection of facial recognition information in digital public spaces by private entities shall adhere to the principle of informed consent. While facial images may be publicly available on the Internet, this does not imply that private entities can extract and collect such information without obtaining informed consent. Sharing a photo with facial images does not automatically grant consent to data processors, such as platform providers to utilize facial recognition technology to identify individuals within that image (Selvadurai, 2015). The uploader's consent to upload photos does not negate the requirement to seek consent from the individuals depicted in the photo for the collection of their facial information. It is recommended that the intended purpose of facial recognition information collection be communicated to data subjects, and their consent shall only be valid for the specified purposes and not beyond those (Chan, 2021). Other principles include the principles of reasonable and clear purpose, necessity, and data minimization. It means that any acts of processing personal information in public spaces must have a clear and valid purpose. The processors should adhere to this purpose consistently. Necessity refers to the act of processing personal information being necessary. The principle of minimization requires that processors only collect the minimum amount of information necessary to carry out

their operations. In other words, the information that has been collected shall be sufficient and appropriate for the intended objectives. This principle also mandates that data processors take measures to restrict the amount of personal information they collect from individuals, as well as delete any unnecessary information that is no longer required and establish time limits for data retention (Malek, 2021). The courts would exercise their discretion to apply these principles to address the new issues. The initial step involves scrutinizing the purpose of processors to ascertain its legitimacy. Subsequently, the principle of necessity is applied to determine whether the collection of facial recognition information is appropriate and necessary. There shall be no alternative methods for its collection. The most intricate step entails the principle of data minimization, which mandates that the scale of facial recognition information collection be limited and that the benefits and harms of such collection be balanced. If all these steps are met, it is presumed that the collection is conducted in a legitimate and proportionate manner. The crux of the application of these principles lies in striking a balance between the interests of processors and the informational privacy interests of data subjects regarding digital facial recognition information.

4.1.2. Establishing a Detailed Online Self-Regulation Guidance

In accordance with the user agreements and privacy policies provided by online data processors, such as online platform providers, users are permitted to access a wide range of online services only upon their consent to all applicable conditions. One such condition pertains to the consent of data subjects to the collection of facial recognition information. While the collection of facial recognition data may not be necessary for all of the platform providers' activities, they restrict the scope of their services if data subjects do not provide consent for the acquisition of their facial recognition information. The consent of data subjects is obtained under coercive circumstances. Coercive means in any form do not constitute voluntary consent. In response to issues about coerced consent, it is proposed that mandating facial recognition information collection as a prerequisite for accessing services or products, coupled with coercive or indirect means of compelling consumers to grant authorization, constitutes involuntary actions. Furthermore, platform providers who subsequently utilize facial recognition information are subject to limited activities. Adhering to the principle of purpose limitation, only those whose original intent for collecting facial recognition information is to provide online services are permitted to process it. Consequently, other entities that could

potentially access the data are not authorized to collect the information. This measure effectively safeguards facial recognition information from unauthorized acquisition or misuse. Last but not least, it is commonly observed that the content of user agreements and privacy policies is excessively tedious and unintelligible, leading users to disregard the terms carefully. To facilitate user consent and notification, it is recommended that user agreements and privacy policies be simplified and made easily comprehensible. The content should be highlighted in key points to ensure users can quickly grasp the essential information.

4.2. A Flexible Application of the Informed Consent Principle

4.2.1. The Invalidation of the Informed Consent Principle

Despite the legal requirement for informed consent, data subjects still express concerns regarding the completeness of this requirement by data processors. Obtaining consent for facial scanning and extraction, which involves biometric facial information that is inherent to individuals, is challenging and impractical. This enables data processors to circumvent the consent acquisition process and request data subjects' cooperation more easily. Data subjects' facial images are captured and collected unconsciously in physical public places. A common phenomenon is the installation of CCTV cameras with facial recognition functions by private entities in numerous public spaces without conspicuous notification or with notification that conceals the actual purpose of recognition or identification. In digital public spaces, consent of the data subject is sometimes compelled by data processors. User agreements and privacy policies provided by Internet platform providers stipulate that users can access a wide range of online services only upon consenting to all conditions. Among these conditions is the consent to the processing of facial recognition information. Although facial recognition information is not essential for all their activities, platform providers restrict the scope of their services if data subjects do not provide consent for the acquisition of their facial recognition information. The consent of data subjects is obtained under duress. Coercion in any form does not constitute voluntary consent. Furthermore, as illustrated in the concerns regarding the collection of facial recognition information in digital public spaces, platform providers may initiate an additional process after collecting the information. This process may involve extracting detailed information from photos or videos uploaded by users for identification purposes, even without obtaining explicit consent. In other words, platform providers gather information for another purpose without specific consent. Sharing

a photo with facial images does not automatically grant consent to platform providers to collect and extract facial recognition information to identify the individuals in that image. The uploader's consent to upload photos does not negate the requirement to seek consent from the individuals depicted in the photo to extract their facial information in detail. This highlights the challenges associated with implementing the consent requirement for data subjects in digital public spaces. Given the invalidation of the informed consent principle in the collection of facial recognition by private entities in public spaces, this article advocates for a flexible application of the informed consent principle.

4.4.2. Standardizing the Requirement for the Informed Consent Principle

This article proposes that before the collection of facial recognition information, data processors shall fully fulfill their obligation to inform data subjects. The notification's content shall be straightforward and transparent, avoiding obscure terminologies and replacing them with plain language to ensure comprehension for the general public. Additionally, the notification shall provide comprehensive information. Given that facial recognition information is a sensitive personal information type, data processors shall inform data subjects in detail about the handling methods, purposes, usage, storage duration, potential adverse effects, owners' rights, information flow, and other relevant details pertaining to the interests of facial recognition information, when they collect facial recognition information. Besides, this article recommends that the principle of written informed consent be applied in China, similar to the requirement of written informed consent in BIPA. Articles 14 & 29 of the PIPL and Article 2 (3) of the judicial interpretation have already required "separate consent" or "written consent" as a prerequisite to collect facial recognition information in the private sector. "Separate consent" or "written consent" emphasizes that an individual shall fully comprehend, clearly express, and voluntarily provide their true intention regarding a separate matter, thereby enabling an individual to genuinely participate in the protection of their information.

4.2.3. Establishing a Dynamic Consent Mode

The initial suggestion starts with scenarios where the collection of facial recognition obtains data subjects' consent. Despite the lawful collection of facial recognition information, data processors may further process and use facial recognition information beyond its initial purpose. The one-time informed consent provided during the data collection does not imply

consent to subsequent processing and usage. Preliminary consent may be interpreted as permanent authorization by data processors, leading to insufficient knowledge about subsequent processing details. This article proposes that the informed consent principle should remain applicable throughout the entire process, including the collection, process, and use of facial recognition information. Due to its limited practical significance for further information processing and usage, the initial consent obtained during the data collection stage alone may not adequately safeguard individuals' facial recognition information. Therefore, a dynamic consent mode requiring continuous consent from the collection to the usage stage would be more appropriate to align with facial recognition information protection. The second suggestion addresses the scenario where data processors collect facial recognition information without obtaining consent. This article suggests that the effectiveness of such information collection without consent should be determined. If data processors adhere to the following two principles, their activities are permissible. The first principle is the principle of purpose legitimacy and consistency. Data processors must ensure that the purposes for which they collect data subjects' facial recognition information align with relevant activities and comply with prohibitive laws and regulations. Additionally, the purpose must remain consistent throughout the entire process, prohibiting data processors from altering the original purpose for subsequent processing and use. The second principle is the principle of data minimization. The collection and activities following facial recognition information collection must adhere to this principle. Data processors shall collect, process, and use only the minimum amount of facial recognition information necessary for the purposes of their activities. Upon achieving the purposes of their activities, facial recognition information shall be promptly deleted.

5. CONCLUSION

Facial recognition information is regarded as sensitive and special personal information in China, the EU, and the US. Individuals have the right to informational privacy regarding their facial recognition information. Given the relatively less intrusive nature of facial recognition technology, the collection of facial recognition information may be conducted secretly without physical contact with the individual. The illegal collection of facial recognition information in public spaces by private entities would constitute a violation of data subjects' informational privacy

rights. China has established a regulatory framework to regulate the illegal collection of facial recognition information in public spaces by private entities. Inspired by similar forms of regulatory measures implemented in the EU, the mechanism in China has formed with the Personal Information Protection Law as the fundamental, the Regulation on the Administration of Network Data Security (Draft for Comments) (2021), the Information Security Technology--Facial Recognition Information Security Requirement, the judicial interpretation, and the Provisions on Security Management of the Application of Facial Recognition Technology (for Trial Implementation) as supplements. The regulatory framework underwent a gradual evolution, transitioning from a permissive approach to a more restrictive one. While the essence of the Chinese regulation is distinct from the EU's and the US's. Neither does it emphasize the protection of the sacred nature of data subjects' informational privacy rights nor prioritizes the value of the free flow of personal information in the market. Instead, China's regulations concentrate on rules to regulate the specific activities of data processors. Despite recent improvements in Chinese regulations, this article contends that the Chinese pattern is insufficient to protect data subjects' privacy rights regarding facial recognition information. This is primarily due to the loopholes in addressing issues about the illegal collection of facial recognition information in digital public spaces. The article proposes that the general principles of personal information protection could be applied to address online privacy issues in the absence of specific regulations. It also suggests implementing detailed online self-regulation guidance for online data processors, such as online platform providers. Furthermore, this article recommends a flexible application of the informed consent principle, such as standardizing the requirement for the informed consent principle and establishing a dynamic consent mode. It is believed that a more comprehensive regulatory framework could effectively protect data subjects' privacy rights regarding facial recognition information in China.

References

Alterman, A. (2003). ``A piece of yourself'': Ethical issues in biometric identification. *Ethics and information technology*, *5*(3), 139-150.

Berle, I., & Berle, I. (2020). Compulsory Visibility? *Face Recognition Technology: Compulsory Visibility and Its Impact on Privacy and the Confidentiality of Personal Identifiable Images*, 75-85.

Blunt, R., & Schatz, B. (2019). Commercial Facial Recognition Privacy Act of 2019. In.

Carrero, A. (2017). Biometrics and Federal Databases: Could You Be in It. *J. Marshall L. Rev.*, *51*, 589.

Chan, G. K. (2021). Towards a calibrated trust-based approach to the use of facial recognition technology. *International Journal of Law and Information Technology*, *29*(4), 305-331.

Corbit, H. (2022). Face Value: A Proposal for Federal Regulation of Facial Recognition Technology Companies. *Stetson L. Rev.*, *52*, 779.

Dul, C. (2022). Facial Recognition Technology vs Privacy: The Case of Clearview AI. *QMLJ*, 1.

EUROPEIA, C. (2021). Proposal for a Regulation on a European approach for Artificial Intelligence. *Bruxelas: Comissão Europeia*.

Kaur, P., Krishan, K., Sharma, S. K., & Kanchan, T. (2020). Facial-recognition algorithms: A literature review. *Medicine, Science and the Law*, *60*(2), 131-139.

Madiega, T., & Mildebrath, H. (2021). *Regulating facial recognition in the EU: In-depth analysis*. European Parliament.

Malek, M. A. (2021). Bigger Is Always Not Better; less Is More, Sometimes: The Concept of Data Minimization in the Context of Big Data. *Eur. J. Privacy L. & Tech.*, 212.

Mann, M., & Smith, M. (2017). Automated facial recognition technology: Recent developments and approaches to oversight. *University of New South Wales Law Journal, The*, *40*(1), 121-145.

McClellan, E. (2019). Facial recognition technology: balancing the benefits and concerns. *J. Bus. & Tech. L.*, *15*, 363.

Moore, A. D. (2015). *Privacy rights: Moral and legal foundations*. Penn State Press.

Regulation, P. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council. *Regulation (eu)*, *679*, 2016.

Schwartz, P. M., & Peifer, K.-N. (2017). Transatlantic data privacy law. *Geo. LJ*, *106*, 115.

Selvadurai, N. (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.