

The Legal Firewall under the Algorithmic Panopticon: "Precision Regulation" and Privacy Reconstruction of Facial Recognition in Public Places

Jilun Zhu *

College of Arts and Science, New York University, New York, United States

*Corresponding Author: jz5095@nyu.edu

ABSTRACT

There is an increasing use of facial recognition technologies (FRT) in daily life. The privacy invasion created by this technology and the public's growing discomfort with being monitored at all times are having an impact. They are affecting people's ability to feel secure when entering and leaving public places. While this article will not provide a comprehensive list of all laws developed because of FRT, it will explore how society is moving toward new ways of organizing its societal norms and public values. Using the framework of "first principles" reveals how legal systems are developing laws around new and existing technologies; in this specific instance, the article provides examples of the continual existence of the presumption of innocence and the right to be treated equally under the law. Once these principles are analyzed, the article examines how the techniques used to regulate these technologies, such as minimum necessity, edge storage, and quantified filing, are built using institutions and their interrelationships. Using the European Union's and United States' approaches, the article provides a basis for understanding how China is developing an entirely new regulatory framework—exemplified by the Administrative Measures on the Security of Application of Facial Recognition Technology ("2025 Measures")—that provides an appropriate dynamic balance between the collection of personal information for security and the protection of individuals' rights through physical separation and procedural measures.

KEYWORDS

Facial Recognition; Public Places; Privacy Right; 2025 Measures; Algorithmic Regulation

1. INTRODUCTION

Technology is rapidly changing the physical nature of public spaces at a fundamental level. In the past, public spaces were places for social interaction where people could remain anonymous and come and go freely. Today, that environment has changed completely. People are now constantly tracked by monitoring devices placed everywhere. Furthermore, the physical space itself is being turned into a data-driven, artificial environment, meaning people now inhabit a space that is as much digital data as it is physical reality. Facial recognition technology (FRT) has gone from being a tool for identifying individuals to a technology used to govern individuals through how they are managed via the infrastructure level of society. The pervasive nature of technology has led to the breakdown of what is referred to as "civil inattention"—the social norm of politely ignoring others—as the availability of FRT makes it impossible to remain unnoticed; thus, the public environment has become an "algorithmic audit field." In this space, the activities and paths taken by citizens, their social interactions, and their emotional states can all be monitored and evaluated constantly. The

"Panopticon" effect has created a complete reversal of the traditional relationship that exists between citizens and their physical space [1].

The current rights protection system and the rapid growth of technological capabilities have created a gap between them. With deep learning algorithms making it possible to integrate personal locations into digital pathways continuously, the difference between seeing something for a brief second at one point in time, versus continuously gazing at something in real-time, has become drastically altered. Because of this alteration, the concept of "no expectation of privacy in public spaces" has become obsolete. Today's main crisis is not just about data loss; it is about the loss of public privacy. Privacy has been taken away by private businesses and agencies that are using the justification of security and efficiency to take advantage of individuals' biometric data. The line between technology and privacy is blurring more than ever. While individuals benefit from technology's convenience, they give up control of their biometric information, which represents an important part of their identity; the level of conflict and confusion between expectations of technology and privacy in this area is unprecedentedly high at this time [2].

Based on the above background, on June 1, 2025, the Administrative Measures on the Security of Application of FRT (hereinafter referred to as '2025 Measures'), jointly published by China's Cyberspace Administration and Ministry of Public Security, will officially be put into use. The publication of the "2025 Measures" is an indication that the management of FRT in China has moved from the previous stage of "disorderly development" to one characterized by "precision regulation" and "full process supervision". This regulatory mechanism has effectively filled the gaps in the existing laws with regard to the application of FRT, addressing the serious social challenges created by technology through specific institutional design [3]. This article focuses on the "2025 Measures" and compares them with the preventative and litigation models used in Europe and the USA, respectively, to provide a better understanding of the legal limits of using FRT for public and private purposes, and to develop effective methods for protecting personal information in a society increasingly dominated by technology.

2. CRISIS MAPPING FROM THE RIGHTS PERSPECTIVE: FROM TECHNICAL ATTRIBUTES TO LEGAL DILEMMAS

2.1. The Alienation of Evidentiary Validity: From "Deterministic Facts" to "Probabilistic Predictions"

As most people know, biological evidence is often viewed by courts of law as conclusive proof of a person's "identity." Typically, courts will base their judgment of a person as "guilty" or "innocent" on the concrete characteristics of the person's biological evidence. In contrast, the modern use of FRT does not focus on the biological characteristics found in images of a person as being definitive or absolute measures of a person's "identity." While biological evidence can provide some basis for determining who a person is, the matching output produced by FRT today, i.e., the probability that two vectors produce the same output, is fundamentally different from how courts assess "identity" based upon biological evidence. In general, the output produced by FRT is a statistical prediction of whether two vectors match and carries with it a level of confidence. In law enforcement and security, this represents a "probability" of a match. If an officer or manager relies too heavily on the results produced by a FRT algorithm with a high level of confidence, it is common for them to overlook or dismiss any additional circumstantial evidence that may exist. The comparison of the FRT output to an officer's or manager's other sources of identification has the potential to undermine a person's civil rights. Robert Williams is an example of a person who was arrested based solely on a false positive produced by an algorithm. The failure of officers and managers to appropriately consider other circumstantial evidence in determining "innocence," as well as the failure to regulate procedural

errors that occur with technology, threatens the presumption of innocence, which is essential to the rule of law [4].

2.2. The Implicit Erosion of the Right to Equality: Algorithmic Bias and Structural Discrimination

Compared to the challenge of accuracy, the fairness crisis of algorithms strikes directly at the core of the constitutional right to equality. Multiple authoritative technical evaluations show that, limited by the insufficient representativeness of training data and physical imaging characteristics, FRT algorithms show significant "demographic differentials" when processing different groups of race, gender, and age. According to a report by National Institute of Standards and Technology (NIST), under specific algorithmic models, the false positive rates (misidentification rates) for groups such as African American women and Asians are far higher than for white men [5]. This deviation at the technical level, once connected to the large-scale surveillance network in public places, will be amplified into structural discrimination at the social level. Different from traditional human discrimination, this "algorithmic bias" is often cloaked in "technological neutrality" and "mathematical objectivity," being extremely deceptive and concealed. Under the current framework of tort law or the Personal Information Protection Law, victims often find it difficult to prove that they have suffered differential treatment based on algorithms, which causes the protection of the right to equality to face a serious dilemma of proof in the digital age.

2.3. The Hollowness of Informed Consent: The Crisis of "Objectification" in Public Places

Examining legal procedural justice, the "non-contact," "long-distance," and "insensible" characteristics of FRT have caused the traditional "inform-consent" mechanism to completely fail in public places. In physical space, an individual's biological features are passively exposed, which has an essential difference from users actively clicking "agree" clauses in cyberspace. If commercial institutions or managers, without fulfilling sufficient notification obligations, continuously collect and analyze pedestrians' facial features through hidden cameras, it is tantamount to depriving data subjects of their right to know and right of choice. The "gaze" that society uses to view individuals solely from a one-directional perspective implies that citizens are dehumanized and, therefore, are not treated as "subjects of rights" under the law but rather simply as "data objects," enabling algorithms to extract data for analysis. This objectification of human beings violates the right to human dignity guaranteed by civil law and causes psychological damage through the "chilling effect" on the ability of people to act naturally and legitimately without concern for being surveilled. Ultimately, this creates an environment where people are discouraged from participating in the marketplace of ideas, and where their public existence is limited to a dull and uninspired series of interactions with others.

3. INSTITUTIONAL RECONSTRUCTION: THE LOGICAL DECONSTRUCTION OF THE 2025 CHINESE REGULATORY PARADIGM

3.1. The Scene-Based Landing of the "Minimum Necessity" Principle

The "2025 Measures" addressed the limitations of consent mechanisms and further developed the "minimum necessity" principle when creating additional non-exclusive rules regarding the use of FRT. Article 10 of the "2025 Measures" states that if another technology (like a swipe card or QR code) would suffice to achieve the same verification security, then the exclusive use of FRT is prohibited. This ensures that each person is given a choice as to what form of technology they wish

to utilize for verification, while still retaining the option to use FRT if they prefer. In short, while Article 10 prohibits the use of FRT as the sole means of verification, the "2025 Measures" confirm that using Facial Recognition Technology will always be an option, but not the primary or only option. Also, Article 12 of the "2025 Measures" provides a list of places where the use of the technology is prohibited and, therefore, bans the installation of any equipment utilizing FRT. These include an individual's private areas such as hotel guest rooms, public bathrooms, changing rooms, and public restrooms. Thus, such clear spatial definitions and limitations reflect the concept of "private places" within the confines of a digital world.

3.2. The Physical Isolation of Data Governance: From Cloud to Edge

Article 8 of the "2025 Measures" introduces strict technical rules for handling facial data. It requires that this data be stored directly on the device (the terminal) rather than being sent over the internet [3]. There are only two exceptions to this rule: if a specific law requires otherwise, or if the user gives separate, explicit consent. The edge storage requirement allows the legal system to reshape the technical architecture of FRT systems by moving away from "cloud aggregation" toward "edge computing." The legal benefit of edge storage is that it greatly reduces the systemic risk of large volumes of FRT data leaking from a single point. If one terminal device is hacked, the only information exposed is the data stored on that terminal device, and not the data stored on a cloud database that may contain millions of records. The governance philosophy of "keeping data with the person" demonstrates a shift in legislative philosophy from "punishing after the fact" to "preventing at the source." This enhancement of the security baseline of FRT applications within public areas has led to greater confidence in the continued use of FRT.

3.3. Quantified Regulation: The 100,000-Person Filing Threshold

To tackle the challenge of the power imbalance between agencies and companies using new technologies to create profits (through asymmetric regulation), Article 15 of the "2025 Measures" includes a quantitative regulatory standard. When the use of FRT results in the storage of personally identifiable information of more than 100,000 people, the organization must submit a report to the provincial cyberspace regulatory authority [3]. This establishes a significant classification policy, bringing large chain organizations (data monopolists) into a defined space of regulatory scrutiny and increasing compliance costs, while requiring them to adopt a prudent approach. This policy also provides an objective "de-stocking" strategy, creating a financial burden for large data retailers that will ultimately reduce their profit margins. To avoid cumbersome filing procedures and strict substantive reviews, many small and medium-sized enterprises (such as single residential district property management, small supermarkets) will actively establish periodic data deletion mechanisms to cleanse long-term inactive "zombie data" and control the storage volume below the red line. This mode of forcing data lifecycle management through administrative procedures effectively curbs the impulse of enterprises to hoard facial data without limit.

4. COMPARATIVE LAW PERSPECTIVE: THREE PATHS OF GLOBAL REGULATION

Projecting China's regulatory practice onto the global coordinate system, its institutional positioning becomes clear at a glance. Currently, major global jurisdictions have formed three typical paths in the governance of FRT in public places.

4.1. The EU Model: The Risk-Based "Precautionary Principle"

The EU has adopted the world's most radical "precautionary principle" path. The Artificial Intelligence Act (EU AI Act) passed in 2024, in Article 5, explicitly classifies the use of "real-time"

remote biometric identification systems (RBI) in public places for law enforcement purposes" as an "Unacceptable Risk," and prohibits it in principle [6]. Although the Act retains "absolute necessity" exceptions for extreme situations such as terrorist attacks and searching for missing children, its legislative logic is based on the absolute priority of fundamental rights. The EU model attempts to fundamentally block the possibility of technology abuse by setting legal forbidden zones; it has a strong color of human rights protection, yet inevitably sacrifices the efficiency of public security governance.

4.2. The US Model: Judicially Driven "Post-Event Relief"

Distinctly different from the EU, the United States lacks unified privacy legislation at the federal level, and its regulation mainly relies on scattered state laws and judicial precedents. The Illinois Biometric Information Privacy Act (BIPA) represents state laws that allow individuals to file lawsuits for unauthorized collection of their biometric information (e.g., fingerprints, FRT), and this has resulted in a number of large class actions against companies like Clearview AI for compensation [7]. Federal courts have used constitutional precedents (Carpenter case) to progressively extend the logic of the Fourth Amendment prohibiting unreasonable searches to include new technology and digital surveillance [8]. The way in which the US model operates provides only a mechanism for "post-event relief" to the extent of imposing "costly litigation" on infringing companies and creating a fragmented body of law, thereby providing a low degree of legal certainty for businesses and individuals.

4.3. The Uniqueness of the China Model: Administration-Led "Precision Regulation"

The unique approach taken by China is referred to as the China model. Contrary to the EU's all-encompassing ban, or the US's total reliance on litigation after events, the "2025 Measures" have taken an entirely different route by creating an administration-led segmentation of scenes and ongoing supervision over the course of all stages of development. The filing system, labeling obligations, and security assessments allow China to define in detail what is expected for the use of technology without discounting its potential for security benefits. The key component of the China model is that the responsibility for securing data lies with the state and is consistent with the governing philosophy of "coordinating development and security." While protecting the privacy baseline, the China model does not seek to prevent or delay new technological innovations.

5. EMPIRICAL EVIDENCE OF LEGAL BOUNDARIES IN TYPICAL SCENARIOS

In order for any law to realize its life and purpose through application, however, the legal status of using FRT in public places is defined more narrowly through specific dispute cases stated within the framework of the "2025 Measures".

5.1. Residential Districts: The Game between "Access Control" and "Property Rights"

Residential districts are the "semi-public spaces" where FRT contradictions are most concentrated. In judicial practice, typical "cases of homeowners suing property management to delete faces" have established important adjudication rules. Courts hold that homeowners enjoy ownership rights over the exclusive parts of the building, and entering and exiting the district is a necessary extension of exercising property rights. As service providers, if property management companies forcibly set FRT as the sole method of passage, it not only violates the "separate consent" rule regarding the processing of sensitive personal information in the Personal Information Protection Law, but also constitutes a substantive obstruction to the homeowners' property rights [9]. Therefore, the legal boundary is extremely clear: even for district security, property management must provide alternative solutions

such as IC cards or manual passage. Convenience must never become an excuse for depriving the right of choice, and the will of the majority (such as resolutions of the owners' committee) also cannot override the statutory privacy rights and interests of the minority.

5.2. Hotels and Tourism: Farewell to "Forced Face Swiping"

In the hotel scene, the long-existing phenomenon of "forced face swiping" met its end in 2025. Previously, some regions, on the grounds of "public security management," required travelers to undergo facial comparison in addition to ID card verification. However, according to the "minimum necessity" principle of the "2025 Measures", examining identity documents is sufficient to meet the statutory requirement of confirming identity, and extra forced face swiping belongs to "excessive demand for authority." Policies subsequently issued in places like Shanghai and Hangzhou explicitly cancelled this mandatory provision, returning to the "ID card + manual verification" mode [10]. The clarification of this boundary delineates the boundary between commercial operation rights and administrative management rights, making it clear that when there is no explicit legal authorization, commercial venues shall not collect biological features without authorization in the name of "cooperating with law enforcement."

5.3. Commercial Retail: "Insensible Capture" and "Killing the Familiar"

Pure commercial venues such as shopping malls and sales offices using FRT for "insensible capture" to analyze customer flow or identify VIP clients have been explicitly defined as illegal acts. Such acts are usually conducted without the customers' knowledge, strictly violating the requirements of "conspicuous labeling" and "separate consent." The fact that some business owners are using face prints and facial information to link their historic purchase data to enable "big data price discrimination" for specific users is not only a violation of privacy rights but also violates Section 8 of the Implementing Regulations for the Law on the Protection of Consumer Rights and Interests in terms of fair trading practices [11]. Therefore, the legal boundary here manifests as the "blocking of commercial purposes": unless extremely high-standard informed consent is obtained, commercial institutions shall not conduct facial data processing for the purpose of identifying specific natural persons in public areas.

6. DISCUSSION: LEGISLATIVE REFLECTION AND GOVERNANCE APPROACH

Although the "2025 Measures" have constructed a relatively perfect regulatory framework, facing the rapid iteration of technology, we still need to conduct deeper reflection at the legislative and governance levels to deal with unknown challenges.

6.1. Moving Towards the Legalization of "Adversarial Privacy"

In the digital era of the panopticon, relying solely on legal protection may no longer be enough. Establishing the citizens' "right not to be identified" is imminent. This means the law should explicitly protect the right of citizens to take passive defensive measures (such as wearing masks, special patterned clothing, using adversarial stickers) to interfere with FRT systems. In public places, this "adversarial privacy" behavior taken to protect one's own biometric privacy should not be regarded as suspicious behavior or obstruction of official duties. Endowing citizens with the right to remain "invisible" in physical space is the last physical line of defense for resisting algorithmic hegemony and preserving human dignity [12].

6.2. Establishing a Mandatory Algorithmic Audit System

Addressing the "algorithm black box" and "structural discrimination" problems mentioned in Chapter 2, relying merely on post-event tort relief is inefficient. A mandatory algorithmic audit system must be established, requiring all FRT systems deployed in public places (especially systems involving public security and law enforcement) to regularly accept third-party independent testing similar to NIST standards. The focus of the audit should not be limited to identification accuracy rates but should more so include the analysis of differences in false positive rates for different groups of race, gender, and age [13]. The law should mandatorily require the audit results to be disclosed to society to accept public supervision. Only transparent algorithmic audits can cut off the social injustice brought by algorithmic bias from the source.

6.3. Strict Restriction of the Boundary of "Public Security"

"Public security" is often the Sword of Damocles hanging over the right to privacy. To prevent it from alienating into a universal excuse for abusing technology, strict restrictive interpretations must be made regarding "public security" exceptions in judicial practice. According to the principle of proportionality, only when responding to urgent, substantive security threats (such as terrorism, serious violent crimes) is the initiation of large-scale real-time FRT permitted. For general administrative management (such as traffic violations, littering) or commercial security (such as preventing theft), the public security clause should absolutely not be invoked to exempt the "separate consent" obligation. The law must ensure that the penetration of public power into citizen privacy is kept to a minimum, strictly preventing the "pan-securitization" of society from leading to the comprehensive atrophy of free space [14].

7. CONCLUSION

The Chinese government's establishment of the "2025 Measures" demonstrates that the country has established a robust legal barrier for the protection of biometric information. These new guidelines not only eliminate the confusion caused by "forced face swiping" but also effectively revert FRT to its original intended use (i.e., as an "auxiliary tool"). This is achieved through two means: (1) requiring that the use of this technology meet the "minimum necessity" standard and (2) requiring that separate consent be obtained for both the collection and the use of FRT from individuals. In relation to public places, the line drawn by these new laws is very clear. No amount of commercial convenience justifies the violation of an individual's privacy or dignity. Nor can the use of FRT be justified solely by public security concerns. Through the continued implementation of the filing system and the constantly evolving guidance provided by judicial precedent, a new social environment will emerge. This environment will be characterized by more transparent, restrained, and secure uses of FRT data. This will provide the best evidence of a dynamic balance between the rational use of technology and the legal means of achieving that goal in the digital age.

REFERENCES

- [1] Sharon, T., Koops, B.J. (2021). The Ethics of Inattention: Revitalising Civil Inattention as a Privacy-Protecting Mechanism in Public Spaces. *Ethics and Information Technology*, 23(3), 331–343.
- [2] Nissenbaum, H. (2009). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford University Press.
- [3] Cyberspace Administration of China, Ministry of Public Security. (2025). Administrative Measures for the Security of FRT Application. https://www.cac.gov.cn/2025-03/21/c_1744174262156096.htm
- [4] American Civil Liberties Union. (2024). *Williams v. City of Detroit: Settlement Agreement*. <https://www.aclu.org/cases/williams-v-city-of-detroit-face-recognition-false-arrest>

- [5] Grother, P., Ngan, M., Hanaoka, K. (2019). Face Recognition Vendor Test (FRVT): Part 3, Demographic Effects. National Institute of Standards and Technology, Gaithersburg, MD.
- [6] European Parliament, Council of the European Union. (2024). Regulation (EU) 2024/1689 Laying Down Harmonised Rules on Artificial Intelligence. Official Journal of the European Union. <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>
- [7] Illinois General Assembly. (2008). Biometric Information Privacy Act (740 ILCS 14). <https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57>
- [8] Supreme Court of the United States. (2018). Carpenter v. United States, 585 U.S. 291. https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf
- [9] People's Daily Online. (2025). Must Owners Swipe Their Faces to Enter the Community? Court Rules Against Property Management. <http://society.people.com.cn/n1/2025/0726/c1008-40530009.html>
- [10] China News Service. (2025). “Mandatory Face Swiping” Regulated: New Measures for Facial Information Security Protection. <https://www.chinanews.com.cn/gn/2025/04-10/10397093.shtml>
- [11] DeHeng Law Offices. (2021). Is Big Data “Price Discrimination” Really “Fraud”? <https://www.dehenglaw.com/CN/tansuocontent/0008/022054/7.aspx>
- [12] Marx, G.T. (2016). Windows into the Soul: Surveillance and Society in an Age of High Technology. University of Chicago Press.
- [13] Raji, I.D., Gebru, T., Mitchell, M., Buolamwini, J., Lee, J., Denton, E. (2020). Saving Face: Investigating the Ethical Concerns of FRT Auditing. In Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society, pp. 145–151. <https://doi.org/10.1145/3375627.3375820>
- [14] Meng, J., Yin, K., Tian, Z., Ji, W. (2025). From Principles to Details: Revisiting China's New Regulatory Framework for Video Surveillance and FRT. Global Law Office. <https://www.glo.com.cn/Content/2025/09-02/1149417519.html>