Beyond Consent: A PPP-Based Governance Framework for the Legal Regulation of Facial Recognition in Public Spaces

Ziye Wang
School of Foreign Languages, Shanghai Jiao Tong University, Shanghai, China

Abstract: The ubiquitous Facial Recognition Technology (FRT) in public infrastructure has brought on the structural collapse of the "notice and consent" paradigm. In structural environments, consent has become illusory due to asymmetric power and functional expansion. In order to address this systemic lack of legitimacy, this study argues that it is insufficient to gradually improve frameworks based on individual rights, and further a regulatory paradigm shift grounded in Public-Private Partnership (PPP) is put forward. By reconceptualizing biometric data as a quasi-public asset, the author hypothesizes a dual mechanism integrating risk allocation and revenue sharing, to provide a potentially more viable alternative to the challenged consent-based models. Under this mechanism, technological risks can be internalized through contractual liability, mandatory algorithmic insurance, and residual state responsibility. Equally important, data-derived value can be partially recaptured through a data premium tax, and be reinvested via a public interest data trust. Through a comparative analysis of China, the UK, and the U.S., the framework proposed here suggests a modular and transferable approach, which is capable to embed accountability and distributive justice into FRT governance.

Keywords: Facial Recognition Technology; Public-Private Partnership; Biometric Data; Quasi-Public Asset; Algorithmic Governance

1. Introduction

Modern data protection laws mostly rely on a fundamentally liberal premise: the right to informational self-determination [1]. Unfortunately, the deployment of Facial Recognition Technology (FRT) in public spaces is undermining this premise. Unlike discrete data transactions, FRT operates within "environments of structural dependence." In these conditions, individuals cannot really refuse participation, otherwise they have to sacrifice access to essential services and social participation [2].

In this context, consent becomes both mandatory and illusory. As Li (2025) [3] has observed, the integration of FRT into public infrastructure creates asymmetrical power relations in which individuals lack bargaining power which is in fact meaningful. To make things worse, the problem is compounded by the passive nature of consent mechanisms—signages and default enrollments fail to ensure genuine autonomy [4]. When a smart gate is the only entry point to their workplace or home, individuals do not have the freedom to "opt-out". Instead of actively agreeing, they are forced to acquiesce.

Furthermore, owing to function creep, the legitimacy of consent may be further eroded [5]. Frequently enough, data collected for security purposes is repurposed for commercial analytics or cross-platform profiling. This extends far beyond the original context of collection. This temporal instability renders initial consent normatively hollow [6].

Relevant concern is increasingly reflected by judicial developments across the world. In the case Bridges v South Wales Police [2020] EWCA Civ 1058, the Court of Appeal responded strongly to live facial recognition. They held that lacking sufficient legal safeguards and foreseeability, the deployment is deemed to have violated privacy rights. Similarly, in the U.S. Rosenbach v Six Flags Entertainment Corp. case, the Illinois Supreme Court redefined what constitutes a legal injury. The court pointed out that mere loss of control over biometric data, even in the absence of tangible harm, constitutes a legally cognizable injury. This judicial skepticism also occurs in China. Guo Bing v Hangzhou Safari Park (2019) highlights resistance to forced face scans. The court ultimately ruled mandatory biometric collection in commercial settings as a violation of law.

These developments reveal a deeper structural

issue that we must pay attention to. Consent is no longer a viable legitimizing mechanism for FRT governance. Exploratively, this study argues for a paradigm shift, from consent-based regulation to a systemic Public–Private Partnership (PPP) theory-based governance model, treating FRT as a form of digital public infrastructure.

2. Literature Review

2.1 Regulatory Approaches to Data Protection

Different countries have different data protection regimes, indicating divergent legitimization approaches for data processing. In the framework of European Union's General Data Protection Regulation (GDPR), it emphasizes the concept of "legitimate interest", and even allows for data processing without explicit consent under certain conditions. Similarly, China's Personal Information Protection Law (PIPL) introduces the "public security necessity" principle. It permits data collection for public safety purposes [7].

These frameworks have actually expanded beyond consent-based models, and largely focus on legal justification, rather than institutional governance. It's worth noting here that they almost always neglect private actors in public data infrastructures, especially in PPP arrangements.

2.2 The Algorithmic "Black Box" Problem

Algorithmic decision-making opacity is another major challenge we must face. Sun and Liu (2025) [8] highlight the "black box" nature of FRT systems. The black box hinders accountability in bias and error detection, over which the public has no idea. While scholars have advocated for third-party auditing mechanisms [9], these proposals are unfortunately not fully linked to contractual governance. Such partial connection undoubtedly limits their practical effectiveness.

2.3 Traditional PPP Risk Allocation

Traditional PPPs have been the backbone of infrastructure development. In large-scale infrastructure projects such as highways, energy systems, and public utilities, various PPP models have been adopted for the purpose of financing and managing [10]. One of the core principles of the PPP theory is to allocate risk to the most capable party. Ye (2013) [11] pointed out that, effective PPP contracts assign construction, financial, and operational risks to private partners, but retain regulatory oversight within the public sector at the same time.

What we must pay attention to is that, existing PPP literature focuses on tangible infrastructure risks, such as cost overruns and construction delays, but obviously neglects intangible digital risks and their unique characteristics. In the information age, biometric data replaces physical capital as the primary asset. Digital assets carry social risks like privacy violations and algorithmic bias, which will inevitably impact the entire population, especially marginalized group [8].

2.4 Research Gaps

Studies on data protection, algorithmic accountability and PPP governance keeps growing, yet existing research remains structurally fragmented. It is not sufficient to address the systemic challenges posed by FRT. Current legal frameworks mainly focus on ex post justification and individual rights protection, but neglecting ex ante institutional mechanisms. In particular, there are three interrelated deficiencies in current research. Firstly, the workable models that can translate probabilistic and intangible digital harms into structured forms of legal and contractual responsibility, is deficient. Secondly, the political economy of biometric data is inadequately studied. There is scant attention paid to how the enormous economic value generated by large-scale data aggregation should be distributed between private actors and the public. Thirdly, there is a lack of an integrated institutional framework capable of coordinating public and private actors. This results in a governance vacuum. Accountability is diffuse, and often evaded.

In summary, these limitations indicate that incremental improvements within the consent-based paradigm are insufficient. A structural reconstruction of governance logic is needed. It should be able to allocate both technological risks and the value derived from data. Therefore, the author will propose a PPP-based framework in the following section. The new framework will be built around a risk-revenue dual mechanism, and aimed at embedding accountability and distributive justice in the governance of FRT.

3. A PPP-Based Framework for FRT Governance

In this section, the author proposes a dual-track mechanism for FRT governance. It integrates risk allocation and revenue sharing within the contractual framework of PPP. This bold approach attempts to transcend the traditional binary opposition of "government control vs. private innovation" and shift towards a model of shared responsibility and mutual benefit.

PPP is not a unitary model, but includes a variety of contractual forms, such as Build–Operate–Transfer (BOT), Build–Own–Operate (BOO), and Design–Build–Finance–Operate–Maintain (DBFOM). Considering the nature of FRT systems, including infrastructural and data-intensive, the author primarily aligns with the DBFOM form. Under this form, private entities are responsible for the design, financing, and ongoing operations, while the state retains regulatory oversight and residual control over the system. FRT deployment is characterized by ongoing, data-driven, and service-oriented. DBFOM is capable to capture all these characteristics, compared to asset-transfer forms such as BOT. It has the greatest potential of supporting the dynamic algorithmic risk allocation and flexible revenue sharing.

3.1 Risk Allocation: From Liability Avoidance to Shared Accountability

The track of “risk allocation” targets the negative externalities of FRT deployment. These risks include but are not limited to misidentification, discrimination, and privacy violations. It is not a good strategy to treat them as incidental failures. If we can conceptualize them as systemic costs, the risks must be internalized within FRT’s institutional design.

Within a DBFOM-type PPP structure, the private actors are mainly responsible for the design and operation of FRT systems. They are placed in the best position to manage technological risks. But it is precisely for this reason, some firms may utilize information asymmetry to cut spending on risk safeguards. Their natural profit-driven motives even widen the gap between private gains and social costs. The framework addressed here combines strict liability and market-based risk pricing, and consequently reallocates risks to the parties that can best control it.

3.1.1 Strict Liability and Contractual Risk Allocation

Technical risk can be transferred by imposing strict contractual liability for contract breaches. PPP contracts shall explicitly assign data security duties, including but not limited to encryption, access control, and routine system maintenance, to the private partner. In the case of data breaches or unauthorized disclosures, an existing strict liability regime can promptly address them. Penalties must be set according to the sensitivity of biometric data. The more sensitive the data is, the higher the penalties will be. This aligns with the logic of the Illinois Biometric Information Privacy Act (BIPA). Existing research indicates that statutory compensation under BIPA can achieve robust data governance [12].

Concretely, the liability specified in PPP contracts can be risk allocation clauses, performance-based standards, and penalty mechanisms. These rules must be measurable, using the indicators such as error rates, bias metrics, and data protection breaches. Thus, they enable continuous supervision of risk responsibilities throughout FRT’s lifecycle in a DBFOM setting.

3.1.2 Algorithmic Risk Insurance

Supplementally, this framework suggests mandatory algorithmic liability insurance. Private firms must obtain insurance coverage for risks, such as misidentification and bias. With the help of actuarial pricing, insurance markets are capable to qualify the technological risks that are hard to evaluate in advance, and then translate them into quantifiable financial costs. By this approach, firms appropriately internalize the externalities of risks.

The framework leverages insurers as private, informal regulators. Under their influence, firms will have the willingness to adopt safer technologies and governance practices, in order to secure lower premiums. At the same time, insurance schemes ensure timely compensation for harmed individuals. This promisingly improve both efficiency and fairness in overall risk distribution.

3.1.3 Dynamic Risk Governance under PPP

Strict liability and insurance mechanisms form a hybrid of legal and market regulation. Under this mechanism, private actors assume operational risks, while the state retains oversight and intervention powers. Exceptionally, in some high-risk contexts, e.g. public security surveillance, public authorities can never fully

outsource responsibility for rights violations. The government must retain partial liability as the ultimate data steward.

The government bears fiduciary obligations to protect public interests. When systemic failures arise, the state should step in and address them through government-led redress mechanisms. Formal PPP partnership contracts should include robust termination clauses, so that the state may reclaim control if serious violations occur in cooperation.

This approach shifts FRT governance from reactive response to preventive system management. Risks are priced, monitored and redistributed within the proposed framework. It aligns private incentives with public welfare, and potentially forms a key pillar of the PPP-based governance architecture.

3.2 Revenue Sharing: From Data Extraction to Public Reciprocity

The track of "revenue sharing" focuses on the economic dimension of FRT governance. The author proposes a "data premium tax" on secondary commercial uses of biometric data, and furtherly tax proceeds directed into a "public interest data trust". The trust should be managed by independent trustees for principle of fairness, and the purpose of it is to fund third-party algorithmic audits and privacy advocacy. This model draws on the principles of natural resource governance. It treats public biometric data as a quasi-public asset, thereby enhancing its normativity and policy rationality.

Biometric data aggregation exhibits non-rivalrousness and partially non-excludability. It generates operating dynamics, similar to public goods in practice. Pure market forces carry the risk of leading to insufficient safeguards and excessive value extraction. It is necessary to help correct such problems by structured public intervention via PPP.

3.2.1 Biometric Data as a Quasi-Public Asset

FRT systems derive value from large-scale public biometric data aggregation. With these datasets expand, their utility becomes increasingly collective. Essentially, public biometric data resembles infrastructural resources rather than purely private assets [13]. The network effects further raise the marginal value of large-scale data. Since part of the economic benefits is generated by social participation, the generated value is not fully attributed to private investment alone. This supports the classification of biometric data as quasi-public assets.

3.2.2 Data Premium Tax

Based on the discussion above, a data premium tax imposed on firms profiting from secondary data uses is necessary. The tax applies only when firms meet the regulatory compliance standards of algorithmic auditing, purpose limitation and data protection standards. Its economic justification lies in rent extraction: part of such profits comes from data rents rather than pure technological innovation. With tiered tax rates set for more intrusive or commercially intensive uses, the mechanism captures and redistributes the surplus value. By redistributing public data value in line with principles found in natural resource governance, the mechanism does not legitimize data exploitation, but rather conditions and corrects it.

3.2.3 Public Interest Data Trust

Tax revenues should be channeled into a public interest data trust for special use. Under independent governance, the trust funds oversight audits and protection measures for vulnerable groups. It also corrects negative externalities like algorithmic bias, misidentification, and privacy harms. Funding for supervision helps internalize external costs in FRT governance. In addition, an independent body should manage the trust with clear fiduciary responsibilities. This may effectively prevent regulatory capture and opportunistic fund abuse.

4. Comparative Perspectives: A Functional–Contextual Analysis of PPP-based FRT Governance

A functional–contextual comparative approach is adopted to analyze PPP-based FRT governance in this section. Functionally, the author identifies three core regulatory tasks in FRT governance, which are deployment legitimacy, technological risk allocation and data-derived value distribution. Contextually, the author explains how different institutional environments shape distinct regulatory priorities. Focusing on China, the UK, and the U.S. with distinct governance logics, the analysis here does not evaluate regimes in isolation from one another, but treats them as partial institutional responses, inspiring for a more integrated design.

4.1 China: Administrative Legitimacy and the

Externalization of Algorithmic Risk

China's regulatory framework is centered on administrative authorization under the PIPL. As people experience in their daily lives, FRT has been embedded into public security and smart city governance system. This provides a clear administrative basis for lawful deployment.

Nevertheless, risk allocation in public–private cooperation remains poorly defined in the system. This is unfortunately a structural limitation. Though private firms design and run FRT systems in most practical scenarios, liability for errors, breaches and rights violations remains unclear. Judicial interventions, such as Guo Bing v Hangzhou Safari Park (2019), are case-specific, and rarely establish stable, systemic accountability rules.

The proposed framework introduces mandatory algorithmic liability insurance as a solution. At present, though fully developed insurance products remain limited due to actuarial uncertainty, cybersecurity insurance practices hint at a workable implementation approach. Risk pricing is closely correlated with measurable indicators, including but not limited to error rates, audit results, and model transparency. Differentiated premiums can certainly reduce problems of adverse selection and moral hazard.

This approach turns uncertain technological harms into quantifiable and therefore insurable financial risks. It not only ensures compensation for those harmed by algorithmic failures, but also encourages firms to improve safety for more favorable insurance terms. In this way, China's model is believed to move toward market-mediated risk internalization.

4.2 United Kingdom: Rights-Based Accountability and the Limits of Regulatory Jurisdiction

The UK follows a typical rights-based governance model. The PPP-based FRT governance is based on Article 8 of the European Convention on Human Rights (ECHR) and proportionality principles. The Bridges v South Wales Police case reflects this judicial oversight logic.

The UK system performs well in securing procedural accountability, and FRT deployment faces consistent judicial and regulatory scrutiny. Regrettably, there is no effective tools for governing biometric data economics, thus the distribution of value from large-scale aggregation remains unaddressed.

The proposed framework suggests a data premium tax on secondary commercial uses, and tax proceeds directed into a public interest data trust. Although these suggestions probably raise concerns about the impact of innovation, these challenges are institutionally manageable. The tax should apply only to profits from secondary commercial activities such as behavioral analytics, and public-security functions would remain outside its scope in most cases. Tax rates can be adjusted based on data sensitivity and intrusiveness levels. The more commercially exploitative the context is, the higher the rates are.

Such a tax mechanism targets data-driven economic rents rather than primary innovation, which will not hinder creativity, and when revenues are reinvested into oversight, it may strengthen long-term market trust. Accordingly, this may extend the UK model toward greater economic fairness in governance.

4.3 United States: Liability-Driven Enforcement and the Fragmentation of Governance

The U.S. system relies heavily on ex post liability and private enforcement. BIPA and related cases such as the Meta (Facebook) biometric privacy settlement show that strict liability can internalize risks effectively.

Yet the regime suffers from structural fragmentation in governance. Central coordination is absent in many cross-jurisdictional contexts. Ex ante governance remains weak in public-sector FRT deployments.

Unlike China, the U.S. requires better coordination within a liability system. On the one hand, PPP contracts can set unified compliance standards across state-level regimes, which may encourage informal regulatory convergence without federal legislation. These bring ex ante governance to a reactive system, and consequently mandatory assessments and audits shift regulation toward prevention. On the other hand, the data steward model restores a coordinating public oversight role. This role supports vendor supervision and enforcement integration.

In short, the suggested mechanisms do not replace U.S.'s original liability model, but convincingly makes it more coordinated and institutionally integrated.

4.4 Synthesis: PPP as an Integrative Governance Mechanism

The comparative analysis above reveals a consistent structural pattern across jurisdictions. We see each jurisdiction resolves one dimension of FRT governance, but also leaves others underdeveloped. China gains legitimacy but lacks systematic risk allocation rules; the UK ensures rights-based accountability but ignores value distribution; the U.S. internalizes risk effectively but remains fragmented and reactive. With clear comparisons, we can logically understand these models as functionally complementary but institutionally incomplete. The core features are briefly summarized in Table 1.

Table 1. Comparison of Governance Models and PPP-Based Solutions for FRT

Jurisdiction	Dominant Governance Model	Structural Deficit	PPP-Based Corrective Mechanism
China	Administrative authorization	Unstructured and externalized technological risk	Contractual risk allocation; algorithmic liability insurance; residual state liability
United Kingdom	Rights-based regulatory oversight	Absence of value redistribution and incomplete PPP liability structuring	Data premium tax; Public Interest Data Trust; contractualized risk-sharing
United States	Liability-driven and litigation-based enforcement	Fragmented governance and lack of ex ante coordination	Mandatory insurance; ex ante PPP risk allocation; state coordination via data stewardship

We have to notice that, this framework is not limited to the three jurisdictions discussed, but rather corresponds to three broader regulatory archetypes observable, across legal systems worldwide. China's model is representative of state-centric, infrastructure-driven regimes, such as Singapore and United Arab Emirates. In these jurisdictions, digital governance is closely integrated with public administration. The UK's model reflects a rights-based system, characteristic of European Union countries, such as Germany and France. The U.S.'s model reflects an exemplifier of market-oriented, litigation-driven system. They influence jurisdictions albeit in hybridized forms, such as Canada and Australia.

The proposed PPP-based framework thus acts as a trans-systemic institutional solution. The complete framework combines risk allocation, public accountability and value redistribution. These components form a modular design adaptable to different legal traditions. PPP thus serves not only as procurement, but as an integrative governance device. Its importance lies in aligning legitimacy, accountability and economic justice across systems.

5. Conclusion

This study proposes a shift from individualistic consent-based toward a systemic PPP model for FRT governance. Where consent becomes structurally weak, legitimacy is reconstituted through institutional design: risk is internalized via mandatory insurance, and data-derived value is redistributed through targeted tax and trust mechanisms. By treating FRT as digital public infrastructure, the framework is expected to unify norms and practice. The proposal elevates PPP from a contractual tool to a quasi-constitutional governance device, with embedded oversight and distributive fairness.

The proposed framework is modular in its core design, and offers a transferable toolkit for diverse legal environments. According to specific contexts, risk allocation and value redistribution can be adapted. Although challenges remain in quantifying probabilistic harms and setting fiduciary standards, the model provides a coherent approach to balance innovation and public interest. Expectantly, the legitimacy of public FRT will depend less on formal consent alone, but more on whether risks and rewards are structured and fairly governed.

References

[1]Ehrhardt Jr., Marcos. Challenges to Enforcing Informative Self-Determination under the General Law of Data Protection (GLDP) [J]. Civilistica, 2023: 1-16.

[2]Neil, R., Woodrow, H. The Pathologies of Digital Consent[J]. Washington University Law Review. 2019; 96(6): 1461-1503

[3]Li, B. Legal Problems and Regulations of Face[J]. Dispute Settlement. 2025; 11(7): 87-95

[4]Huo, X., Xue, H., Xu, X., et al. A risk sharing

model for old community renewal project based on bargaining game model[J]. Scientific Reports. 2024; 14(1): 24316-24316.

[5]Valipour, A., Yahaya, N., Md Noor, N., Mardani, A., Antuchevičienė, J. A new hybrid fuzzy cybernetic analytic network process model to identify shared risks in PPP projects[J]. International Journal of Strategic Property Management. 2016; 20(4): 409-426.

[6]Liu, J. Research on the "Informed Consent" Rule in Face Recognition [D]. Shandong University of Finance and Economics, 2025.

[7]Hong, Y. Video Surveillance and Facial Recognition in Public Spaces: International Perspective and Chinese Approaches[J]. Journal of Public Security Science. 2025; 8(6): 39-58.

[8]Sun, M., L, W. The Legal Remedies and Regulatory Approaches for Privacy Protection in the Context of Facial Recognition Technology[J]. Legality Vision. 2025; (30): 4-6.

[9]A. Ng., Martin, L. Risk allocation in the private provision of public infrastructure[J]. International Journal of Project Management. 2007; 25(1): 66-76.

[10]Khwaja, M, M. Review of studies on risk allocation and sharing in public-private partnership projects for infrastructure delivery[J]. Frontiers in Built Environment, 2025, (11): 1-14.

[11]Ye, X., Xu, C. Review and Research on PPP Pattern in China[J]. Soft Science. 2013; 27(6): 6-9.

[12]Chloe, S. Actual Harm Means it is too Late: How Rosenbach v. Six Flags Demonstrates Effective Biometric Information Privacy Law[J]. Loyola of Los Angeles Entertainment Law Review. 2019; 40(1): 51-87.

[13]Han, C. Criminal Law Protection of Citizens' Personal Biometric Information in the Era of Big Data —From the Perspective of Face Recognition[J]. Open Journal of Legal Science. 2023; 11(5): 3991-4000.

