International Journal of Social Sciences and Public Administration
ISSN: 3005-9836 (Print), ISSN: 3005-9585 (Online) | Volume 8, Number 1, Year 2025
DOI: https://doi.org/10.62051/ijsspa.v8n1.09
Journal homepage: https://ijsspa.org

Regulation of Privacy Policies: A Perspective from Public Law Protection of Personal Information

Xiangrui Zhao

Law School, Beijing Normal University, Beijing, China

ABSTRACT

Online platforms process personal data through privacy policies while pledging to protect users' personal information. Although derived from traditional privacy concepts, privacy policies differ significantly in nature-personal information protection carries stronger public law attributes, rendering privacy policies primarily compliance instruments that should integrate both self-regulation and government regulation approaches. With the rapid expansion of platforms' private power, privacy policies, despite their enhanced role, have exhibited alienating effects: failures in self-regulation, erosion of user rights, and circumvention of governmental oversight. To address these issues, a meta-regulatory approach is imperative, requiring tripartite collaboration among platforms, users, and regulatory authorities to refine privacy policy frameworks.

KEYWORDS

Privacy Policy; Personal Information Protection; Self-Regulation; Government Regulation.

1. INTRODUCTION

A privacy policy is a legal document through which online platforms inform users about their personal data processing activities, including collection, storage, and use, while committing to protect such information. In the digital era, data has become a critical production factor whose value grows increasingly prominent. For platforms, aggregating data is essential for optimizing algorithms and enhancing user engagement. Privacy policies serve as the legal foundation for legitimizing the collection and utilization of personal data, coupled with assurances of data protection.

With evolving times, the protection of personal information has witnessed a trend of public law integration in the United States, European Union, and China, with the framework of personal information rights gaining further constitutional theoretical support. Although a privacy policy constitutes a contractual agreement, it increasingly embodies substantial public law elements.

Within the context of personal information protection, data regulatory authorities are progressively treating privacy policies as compliance instruments, advocating for the integration of legal requirements and institutional frameworks into these policies rather than addressing them solely through private law channels. From a regulatory perspective, privacy policies have assumed a dominant discourse position in the self-regulatory domain, wielding significant technical and professional judgment authority through architectural power to govern personal information protection structures.

To mitigate the risks of self-regulatory degradation, proactive government intervention in personal information protection is essential to foster synergistic coordination between self-regulation and government regulation. These practical observations and theoretical discussions provide a foundation for examining personal information protection through a public law lens.

The Personal Information Protection Law of the People's Republic of China (PIPL) has exerted a more direct influence on the regulatory approach to privacy policies. Statutorily mandated dedicated agencies for personal information protection are incentivized to establish communication channels with platform enterprises, safeguard user interests, and drive continuous improvements in privacy policies. Notably, in the broader domain of platform governance, personal information protection has pioneered an administrative-led regulatory model, with legislative orientations at the policy level warranting further scrutiny within public law theory.

This study provides a comprehensive examination of regulatory theories concerning privacy policies within the context of the public law shift. It specifically highlights how platform private power both enables privacy policies and generates alienating effects through its expansion. The analysis ultimately seeks to harmonize the tripartite regulatory forces of platforms, users, and governments through a meta-regulatory approach.

2. INSTITUTIONAL EVOLUTION FROM PRIVACY PROTECTION TO PERSONAL INFORMATION PROTECTION

The concept of privacy policies was introduced into China’s legal domain through the practices of the internet industry, primarily influenced by the U.S. legal framework. In its early stages, the privacy policy model lacked a well-developed discourse on personal information protection. The industry readily adopted the expansive U.S. legal concept of privacy rights, making privacy and its protection the cornerstone of privacy policy design.Under this framework, platforms established the legitimacy of data processing-such as collection, control, analysis, and utilization—through the "notice-and-consent" mechanism, forming a systematic chain of data governance. However, this reliance on privacy-rights-era legal frameworks inadvertently amplified platforms’ data power, granting them a structural advantage over users.As the legal and regulatory landscape gradually shifts toward personal information protection, the traditional privacy protection model has become outdated, failing to address contemporary challenges in data governance.

2.1. Conceptual Distinction between Privacy Protection and Personal Information Protection

Following the enactment of the PIPL, privacy policies have retained their traditional nomenclature in name, but have substantively shifted to a personal information protection paradigm. This evolution from privacy protection to personal information protection reflects not only the rapid development of industry practices necessitating a higher-dimensional regulatory framework, but more profoundly, significant changes in consumers' living conditions in cyberspace. The relatively crude legal concept of "privacy" is being progressively replaced by "personal information."

The right to privacy, which originated in the United States with Warren and Brandeis' seminal 1890 article The Right to Privacy, primarily safeguards an individual's private tranquility and personal space. It presupposes a clear demarcation between private and public spheres, requiring societal respect for personal boundaries and prohibiting unwarranted intrusion into one's dwelling or daily life. As a pre-internet era personality right, the essence of privacy lies in secrecy and freedom from disturbance-allowing individuals to exist outside public scrutiny and remain shielded from improper invasions. In its purest form, privacy constitutes a form of social isolation. [1] In contrast, personal information in the internet age operates differently. When platforms collect users' personal information, they inevitably encroach upon private domains. Users' online activities are constantly monitored by platforms, making the preservation of absolute tranquility and seclusion unrealistic. Therefore, the anonymization of personal information to prevent identification of specific individuals becomes paramount. Personal information is defined as any data that can identify a specific natural

person, and the crux of personal information protection lies in establishing a system of information rights allocation and management mechanisms based on the ownership and control of personal data.

In terms of scope, privacy and personal information overlap-particularly regarding private/sensitive information, which qualifies as both. However, privacy also encompasses numerous non-information aspects, such as the right to undisturbed residence and private activities, which resist precise definition. In contrast, personal information is more concrete: its protective scope is not limited to non-public data; rather, any information identifiable to an individual falls under its purview.

Regarding protection hierarchy, privacy enjoys relatively weaker safeguards, primarily provided by civil law (especially personality rights provisions), with minimal public law (e.g., criminal law) reinforcement. China's Criminal Law lacks standalone privacy offenses; violations implicating privacy are prosecuted under charges like defamation or insult. [2] Conversely, the Criminal Law explicitly criminalizes personal information breaches and information system sabotage, affording personal information higher-dimensional protection.Laws like the Cybersecurity Law of the People's Republic of China, the Data Security Law of the People's Republic of China, The PIPL establish a systematic protection framework, mandating obligations for processors (e.g., collection, storage, deletion) and enshrining user rights. The EU and U.S. have also progressively reformed their privacy protection frameworks through personal information-related legislation to better address contemporary data protection needs. [3] A paradigmatic example is the Charter of Fundamental Rights of the European Union explicitly elevates data protection to the status of a constitutional-level fundamental right. The General Data Protection Regulation (GDPR) has established a comprehensive personal data protection regime that is conceptually and operationally distinct from traditional privacy protection models, significantly enhancing safeguards for personal information.

This transition from privacy to personal information protection reflects a convergence of private and public law approaches, even a shift toward public law dominance.

2.2. The Functional Transformation of Privacy Policies

The PIPL has transformed platform companies' privacy policies from blanket authorization tools for personal data collection into frameworks for defining personal information rights and establishing protective mechanisms. This functional shift in privacy policies serves a dual purpose: First, it compels platforms to actively constrain their personal data collection and processing practices, preventing unlawful use or leakage of personal information while promoting responsible business conduct and prudent operations. Second, it formally recognizes platforms' self-regulatory efforts through privacy policies, incorporating industry best practices to foster collaborative governance between the government and private sector, thereby enhancing regulatory effectiveness. Consequently, privacy policies have gradually evolved into a key compliance instrument for platform enterprises under the law.

More specifically, privacy policies must explicitly delineate users' statutory rights and their corresponding implementation mechanisms. Foremost among these is safeguarding the right to informed consent-users must be able to withdraw consent through an app's privacy settings or opt out of personalized advertising with a single click. For cross-border data transfers, data processors must obtain separate user consent through enhanced disclosure procedures. To facilitate the realization of data portability rights, platforms must establish dedicated customer service channels to support data export functionality. To ensure users' rights to access, correct, and delete their data, platforms must establish robust data deletion mechanisms when personal information is no longer necessary.

To comply with Article 9 ("Security Obligations") of the PIPL, privacy policies must incorporate concrete safeguards. Representative industry practices include: Virtual number systems (e.g., Meituan's masking of real phone numbers in food delivery/hotel bookings, preventing post-service contact by merchants or couriers); Regular risk assessments of sensitive data processing activities

with mandatory remediation of vulnerabilities; Strict oversight of third-party SDKs, including rigorous security audits of their data collection practices.

Conducting online live streaming, e-commerce, and similar business models requires apps' privacy policies to collect users' personal information in compliance with legal and regulatory requirements. For instance, platforms must verify the real identity information of live streamers and fulfill data reporting obligations to the Cyberspace Administration, broadcasting authorities, public security departments, and tax authorities.

The privacy policy must establish a systematic framework for data compliance. Platform companies should set up dedicated data compliance departments to oversee the development of personal information protection rules and ensure regulatory adherence. This includes conducting staff training, implementing data classification and tiered management systems, establishing full data lifecycle governance, and deploying risk monitoring mechanisms.

Given that laws such as the PIPL have already laid out a comprehensive regulatory framework-serving as an institutional blueprint for privacy policies-platform enterprises must continuously refine their policies to align with evolving regulations. Doing so demonstrates their commitment to robust data compliance practices.

3. ANALYSIS OF THE NATURE OF PRIVACY POLICIES

Privacy policies have evolved from mere privacy protection to comprehensive personal data governance. Their regulatory function can no longer be effectively structured through private law autonomy alone. As their contractual attributes diminish, continuing to treat privacy policies purely as contracts renders their operational mechanisms unworkable and may undermine their governance efficacy.

3.1. The Dilemma of Contractual Autonomy

Privacy policies typically require users to check an "Agree" box to access an app's functionalities, formally meeting the contractual elements of "offer" and "acceptance." During the early stages of privacy protection, privacy rights were categorized under civil personality rights, and user consent to privacy policies was viewed as a disposition of personal privacy-trading certain rights for the convenience of online services. Platform companies collect and protect users' personal information through privacy policies, establishing a contractual relationship between the platform and its users. If a platform violates its privacy policy, users may claim breach of contract under contract law. However, critiques of this contractual characterization are equally compelling. Examining the drafting process of privacy policies reveals a fundamental imbalance: although a contract theoretically requires mutual negotiation between equal parties, ordinary users have virtually no say in the terms and can only passively accept them. Privacy policies are unilateral legal documents drafted by platforms to govern the collection, processing, and protection of personal data. [4] Compared to ordinary consumer-users, platform companies-armed with vast resources and capital-hold a dominant position, legitimizing their control over data through the "notice-and-consent" framework while leaving users structurally disadvantaged. Moreover, after the initial "notice-and-consent" transaction, platforms often reserve the unilateral right to modify privacy policies without further user approval. This unilateral amendment power starkly contrasts with traditional contracts and, though ubiquitous in the digital age, lacks a coherent justification-effectively allowing platforms to expand their authority under the guise of contractual terms. Exploiting these asymmetries, platforms frequently minimize their liabilities while restricting user rights. Yet dismissing privacy policies' contractual nature altogether would also be misguided. While contract formation traditionally hinges on mutual agreement, the rise of standardized contracts reflects the impracticality of individualized negotiations in mass-market interactions. Contract law’s progressive role in balancing transactional efficiency (for large-scale

consumer dealings) with cost control should be acknowledged. Rather than fixating on the unilateral and non-negotiable aspects of privacy policies, the more urgent challenge lies in addressing the misalignment between contract law's enforcement mechanisms and the realities of digital governance.

First, users seeking contractual damages from platforms must demonstrate quantifiable losses-a notoriously difficult evidentiary hurdle. While aggregated and processed datasets command substantial market value, individual data points in their raw, atomized form possess negligible economic worth. Platforms typically collect personal information without monetary compensation, rendering traditional damage calculations inapplicable.Infringement of personal information also violates privacy policies, involving the concurrence of liability for breach of contract and tort liability. However, claiming breach of contract is more difficult. Although both tort and contract lawsuits face the challenge of proving damages-and, in many cases, contractual liability may seem more straightforward due to predefined terms, making relief easier to obtain-privacy policies typically do not specify the compensation obligations or amounts for platform companies. This leaves claims for breach of contract without clear contractual support. Moreover, Article 69 of the PIPL establishes a presumption of fault for torts involving personal information, and tort liability allows for compensation of both property and emotional damages, making tort claims a more reasonable approach. Pursuing relief through a breach-of-contract lawsuit would require a more robust legal interpretation to demonstrate the platform's contractual violation and resulting harm-a particularly difficult task given the lack of consensus on the legal nature of privacy policies.

Second, the criteria for determining a platform's violation of privacy policy commitments are ambiguous. For a platform to be held liable for breach of contract, it must violate a specific commitment outlined in its privacy policy. However, in practice, problematic areas-such as expanding the scope of personal data collection, disregarding users' right to informed consent, weakening personal information security safeguards, or leaking personal data-often lack clear enforcement standards. Beyond obvious violations (e.g., failing to obtain separate user consent), most commitments in privacy policies remain vague. For instance, provisions on emergency response mechanisms, security assessments and oversight for sharing data with third parties, or specific procedures for accessing, correcting, or deleting personal information are typically phrased in technical, procedural terms. Some clauses merely reiterate legal requirements verbatim. Consequently, proving that a platform's conduct breaches its privacy policy commitments is exceedingly difficult.

Thus, the contractual nature of privacy policies faces significant challenges in enforcing liability and providing remedies. Relying on contractual autonomy not only encounters theoretical hurdles but, more critically, fails to establish a viable pathway for users to exercise their rights-leaving them trapped in their inherently disadvantaged position against platforms.

3.2. The Public-Law Transformation of Privacy Policies

Internationally, both the U.S. and the EU have primarily relied on self-regulatory frameworks to govern privacy policies. [5] The U.S. has developed a long-standing privacy governance model anchored in constitutional precedents and a specialized enforcement mechanism led by the Federal Trade Commission (FTC). Under the Federal Trade Commission Act, only the FTC has the authority to initiate legal actions against privacy policy violations, as individual lawsuits lack a public-law basis. This approach reflects a key rationale: viewing users as consumers highlights the inherently public nature of privacy policies. Since violations affect not just individuals but the broader consumer base, the FTC acts as a centralized enforcer of organized public interests, rather than relying on fragmented, atomized lawsuits by individual users. Crucially, the FTC acknowledges the significance of privacy policies as self-regulatory tools for platforms. Given the limitations of government oversight, the agency provides broad, principle-based guidance while expecting platforms to actively self-regulate their collection and use of personal data. In contrast, the EU treats personal data protection as a

fundamental right, enshrined in the Charter of Fundamental Rights of the European Union. The GDPR establishes a comprehensive framework for data subject rights, corporate obligations, and legal liabilities. Recent legislation like the Digital Services Act (DSA) and Digital Markets Act (DMA) further imposes stringent platform responsibilities. Unlike the U.S.'s litigation-dependent model, the EU emphasizes proactive administrative enforcement. European regulators frequently launch investigations and impose hefty fines-exemplified by repeated penalties against Meta, as well as actions targeting Amazon, TikTok, and Uber. Privacy policies serve as critical evidence in EU enforcement. For instance, Ireland's Data Protection Commission (DPC) ruled in the TikTok data transfer case that the platform's privacy policy failed to disclose cross-border data flows and remote access, violating GDPR Article 13. It can be seen that law enforcement agencies are precisely comparing the platform enterprises' privacy policies with the GDPR to assess data compliance. Companies are expected to refine their policies accordingly, while regulators actively encourage stricter self-regulation-punishing GDPR violations while recognizing corporate efforts to align with legal standards.

China's personal information protection regime exhibits stronger institutional alignment with the European model, particularly in its administrative enforcement mechanisms. The PIPL establishes comprehensive rights frameworks and information security safeguards, significantly enhancing the public law dimension of privacy policies. Unlike private law remedies, public law instruments are playing an increasingly dominant role in this domain. The Chinese regulatory approach prioritizes administrative governance over individual litigation, as the latter often proves inefficient and cost-prohibitive for systemic risk control. This paradigm manifests in two key aspects: First, privacy policies have evolved beyond their contractual origins to assume substantive public law characteristics. Notably, much of the personal data collection in sectors like live streaming and e-commerce stems from administrative mandates rather than voluntary corporate practices. Second, from a regulatory perspective, platform self-governance represents a more efficient and flexible approach to personal information protection. As the central instrument of self-regulation, privacy policies serve a dual function: they seamlessly integrate personal information management and risk control mechanisms without provoking user dissatisfaction or resistance, while simultaneously enabling the legitimate commercial utilization and value extraction of personal data. This mechanism effectively balances individual rights with corporate interests, establishing a low-cost regulatory framework that coordinates government oversight, platform operations, and user expectations. Such an institutional design inherently aligns with the fundamental objectives and normative principles of public law governance.

3.3. The Synergy between Self-Regulation and Government Oversight

At first glance, privacy policies as a form of self-regulation appear to be platforms' voluntary initiatives to address personal information protection needs and mitigate associated risks through internally designed rules and measures. These policies institutionalize platforms' governance experience into standardized frameworks while leveraging their operational flexibility to develop adaptive safeguards for complex business environments. The conventional view suggests that government regulation operates externally and independently from such self-regulatory mechanisms, with privacy policies primarily serving as platform-driven instruments that reinforce this dichotomy. However, the very concept of self-regulation blurs the line between pure autonomy and varying degrees of government intervention. As noted by Bartle and Vass (2007), regardless of one's theoretical stance, some level of state involvement is inevitable in any self-regulatory regime. [6] The spectrum of self-regulation ranges from complete industry autonomy on one extreme to purely government-mandated compliance on the other, with most practical implementations occupying an intermediate space between these poles. Even in traditionally private domains like family affairs, the protection of women's and children's rights has demonstrated how external regulatory forces inevitably permeate ostensibly autonomous spheres. A self-regulatory approach to privacy policies

that overemphasizes laissez-faire autonomy or pure voluntarism essentially collapses into the contractual autonomy framework. Such an approach risks perpetuating the very limitations that the current personal information protection paradigm seeks to overcome-potentially trapping regulatory design in outdated privacy protection models that fail to meet rapidly evolving data governance demands.

First, the government's recognition of platform self-regulation acknowledges platforms' pivotal role as co-regulators, while maintaining appropriate regulatory boundaries. Platform autonomy proves essential for maintaining ecosystem vitality and fostering orderly market development. The organic, industry-adaptive nature of self-regulatory frameworks enables more responsive market adjustments compared to statutory legislation. However, in the context of personal information protection, privacy policies demand heightened regulatory scrutiny due to their inherent risk exposure. China's legislative prioritization is evident in the early integration of the PIPL and Data Security Law, establishing a foundational governance matrix. This reflects an evolutionary shift from rudimentary privacy safeguards to sophisticated personal information protection regimes, wherein self-regulation must operate within statutory parameters. Notably, the *GB/T 35273-2020 Information Security Technology-Personal Information Security Specification* issued by State Administration for Market Regulation (SAMR) and Standardization Administration of the People's Republic of China(SAC) provides standardized policy templates, exemplifying how government guidance catalyzes self-regulatory advancement. Even in the U.S.-a champion of private-sector-led privacy management-government interventions like merchant certification programs enhance consumer trust in data protection. [7]

Secondly, the self-regulatory nature of privacy policies means that while the 'notice-and-consent' mechanism serves as the legitimizing basis for platforms to collect users' personal information, users remain in a markedly disadvantaged position. Privacy policies are typically lengthy and written in professional jargon, leaving most users without sufficient knowledge or time to thoroughly review them-resulting in perfunctory consent. Users also lack the bargaining power and capability to negotiate specific terms in privacy policies, leaving them no choice but to passively accept the predetermined agreements. Without government intervention in the formulation and modification of privacy policies, unchecked self-regulation could enable platforms to exploit ambiguous clauses to consolidate greater advantage, ultimately abusing privacy policies to systematically exploit users.

Therefore, the synergy between self-regulation and government regulation constitutes the foundational framework of privacy policy governance. Only through their integration can an appropriate balance be struck among the rights and obligations of the three key stakeholders-government, platforms, and users-thereby fully realizing the public law protection of personal information.

4. THE COUPLING OF PRIVACY POLICIES AND PLATFORM PRIVATE POWER

Even as individual rights have expanded significantly in the internet age-evidenced by the rise of "super-individuals" in sectors like live-streaming e-commerce, where key influencers act as critical nodes between consumers and merchants, controlling traffic distribution channels with platform support-ordinary consumers also benefit from easier access to essential services such as food, clothing, housing, and transportation. However, compared to the gains made by individuals, platforms have developed far more rapidly, leveraging technology and self-imposed rules to strengthen self-regulation and institutionalize what can be termed organized platform private power. In the process of collecting and utilizing personal information, platforms amass data resources capable of influencing societal operations, while their private power further reinforces the enforcement mechanisms of privacy policies. Yet, as private entities driven by efficiency, scale, and profit, platforms inevitably experience a drift in public values when acting as de facto regulators. This

necessitates safeguards against the alienation of platform private power-where corporate interests supersede broader societal welfare-to ensure that self-regulation does not undermine fundamental rights and public governance.

4.1. The Multiplicative Effect of Platform Private Power on Privacy Policies

The internet aggregates vast numbers of users, and the larger the user base, the greater the amplification of a platform's commercial value. However, this scale also increases the risk of systemic instability, necessitating mechanisms to prevent user disorder and coordinate collective action. Consequently, platforms assume the role of de facto regulators. A key factor in this dynamic is how platform rules confer governance power over users, enabling platforms to establish and enforce a private regulatory framework. Violations of platform rules can result in sanctions, ranging from content removal to account suspension. Equally significant, though less visible, is the role of user scoring systems-where platforms collect financial, credit, and behavioral data to construct user profiles and facilitate transactions, thereby reinforcing market order. Through content moderation, resource allocation, and punitive measures, platforms wield private power that becomes the cornerstone of self-regulation. This authority is further entrenched by complex feedback mechanisms, where data control and rule enforcement create a self-reinforcing cycle. The result is a multiplicative effect: platform private power not only shapes privacy policies but also magnifies their reach and impact, often without adequate public oversight.

Initially designed to legitimize the collection of personal data, privacy policies served as a contractual basis for users to exchange information for platform services. However, as data protection norms evolved, these policies have assumed an additional function as institutional safeguards-simultaneously preventing malicious actors from misusing personal information while demonstrating platforms' compliance with data governance requirements. This transformation has positioned privacy policies as critical self-regulatory instruments, with platform private power playing a pivotal role in three key dimensions: First, dynamic policy adaptation to sectoral needs.Platforms leverage their institutional agility to iteratively refine privacy frameworks in response to evolving protection demands. While adhering to the baseline standards of China's Personal Information Protection Law (PIPL), they accommodate industry-specific requirements through user feedback mechanisms. By aggregating input from diverse stakeholder groups, platforms optimize their policies to address complex, often competing interests-a capability unmatched by traditional legislative processes. Second, algorithmic enforcement at scale. Regulatory implementation predominantly occurs through machine-driven surveillance rather than manual oversight. Privacy policies, as operationalized through platform rules, rely on automated algorithms to conduct continuous security audits. This system enables a minimal workforce to monitor billions of user interactions, rapidly identifying vulnerabilities and containing potential breaches before they escalate-a feat impossible through conventional governance methods. Third, demand-responsive resource allocation. Sophisticated data analytics allow platforms to decode user characteristics-including purchasing power, behavioral patterns, and social affiliations-into actionable tags. These insights fuel personalized recommendation systems that shape user decisions while enabling targeted content creation. Users themselves harness identity and topic tags to participate in information ecosystems, creating a feedback loop that further refines platform governance strategies.

This demonstrates how platform private power transforms privacy policies from static legal documents into adaptive governance architectures. The integration of real-time responsiveness, algorithmic precision, and granular user profiling creates a self-regulatory regime that simultaneously serves corporate interests and (ostensibly) user protection-though not without inherent tensions between these objectives.

4.2. The Alienation Effects of Platform Private Power on Privacy Policies

While platform private power has enhanced the operational efficiency of privacy policies and optimized resource allocation-thereby strengthening self-regulatory mechanisms-the integration of algorithms and big data has also driven rapid transformations in production paradigms and AI technologies. However, the expansion of platform private power and the application of innovative technologies have simultaneously generated a series of alienation effects.

The first alienated effect is the failure of self-regulation. The self-regulatory framework established through privacy policies may not be rigorously enforced in practice. During the development and operation of technological systems, engineers often neglect security protocols and fail to conduct necessary audits and corrections, thereby undermining the efficacy of self-regulation and rendering it incapable of achieving its intended objectives. First, increased exposure of personal data due to systemic vulnerabilities. When platforms fail to implement adequate data security measures during business operations, unaddressed access loopholes may enable third-party data breaches. The existence of such personal information risk exposure substantially elevates the likelihood of private data being compromised. Second, technical errors in data processing leading to misinformation. Inaccurate algorithmic operations can distort personal data, with significant real-world consequences. For instance, credit information platforms may erroneously conflate two individuals with identical names, incorrectly listing an innocent party as the legal representative of multiple defaulting enterprises. Such errors not only misrepresent individual circumstances but may also trigger unwarranted reputational and financial harm.

The second form of alienation is the erosion of user rights. The bundling of privacy policies with core services locks users into platforms, as basic functionalities become inaccessible without agreeing to those policies. Even though courts have ruled that personal information processors cannot deny products or services on the grounds of users refusing or withdrawing consent to personal data processing, the vast majority of users are still compelled to accept privacy policy terms. Empirical studies confirm that users generally skip privacy policies without careful review. [8] Highlighting key clauses in bold or simplifying language has done little to change the reality that privacy policies remain unread. More critically, even when the Personal Information Protection Law (PIPL) is embedded in privacy policies, vague legal provisions fail to prevent platforms from excessively harvesting personal data due to the abuse of private platform power. On the one hand, the PIPL, as the baseline for privacy policies, cannot fully adapt to the evolving demands of personal information protection in practice. [9] The framework of personal information rights and the protective obligations of data processors rely heavily on privacy policies to "specify general principles into concrete terms," granting platforms significant initiative and interpretive authority. Ambiguous justifications like "improving service quality" or "optimizing user experience" obscure the commercial exploitation of data. So-called anonymized data can still be re-identified through platform profiling. Disputes often involve complex legal interpretations, and if user complaints cannot be resolved swiftly and conveniently, the high cost of exercising rights leads most to abandon their claims. On the other hand, platforms share user data with advertisers and analytics firms through embedded SDKs. Due to data black boxes and the opacity of data-sharing practices, privacy policies rarely disclose third-party data recipients, leaving users unaware and unable to control how their information is disseminated.

The third form of alienation is the marginalization of government authority. The abuse of private platform power seeks to monopolize the allocation and regulatory control of data resources, effectively crowding out public governance. First, the regulatory efficiency of private platform power forces concessions from public authority. Compared to platforms' real-time scanning of billions of data points, government data regulators lack the analytical capacity to screen vast amounts of non-compliant information. As a result, they must rely on cooperation with platforms, delegating the task of identifying violations-such as unauthorized personal data collection-to the platforms themselves. Second, government oversight heavily depends on platform self-regulation. While the Personal

Information Protection Law (PIPL) provides only a broad framework for data protection, platforms de facto dictate the technical standards for safeguarding personal information. Effective public oversight requires active platform cooperation. Moreover, compared to corporate databases, government datasets are inferior in both scale and quality, forcing regulators to frequently request critical data from platforms-further entrenching their dependence. Additionally, laws and regulations permit platforms to verify users' digital identities through facial recognition and the collection of sensitive information. This means platforms increasingly substitute government functions in delivering public services, further eroding the state's role in governance.

5. EXPLORING THE PATH OF META-REGULATION

Given that the expansion of private platform power can lead to a series of negative effects-causing self-regulation through privacy policies to deviate from their intended institutional purpose-it is crucial to tame this private power. While meta-regulation emphasizes the intrinsic value of self-regulation, it does not reject external oversight. Only through tripartite collaboration among platforms, users, and the government can the governance challenges of privacy policies be effectively addressed.

5.1. The Development of Platform Self-Regulation

5.1.1. Fiduciary Duties in Data Trust

The obligations of platforms in data processing should not merely comply with the minimum standards set by the Personal Information Protection Law. Instead, platforms should be encouraged and supported in exploring innovative approaches that better facilitate both data protection and the realization of data value. The theory of data trust can play a significant role in this regard. Professor Jack M. Balkin of Yale University has extended the concept of fiduciary duties-traditionally applied to professionals such as doctors and lawyers regarding client confidentiality-to data processors, terming them "information fiduciaries." [10] Privacy policies should not serve as tools for platforms to exploit their dominant positions. Rather, user trust in platforms must be the foundational premise of self-regulation. Platforms should bear fiduciary duties regarding the commitments made in their privacy policies. When users entrust their personal information to a platform based on the expectation that it will strictly adhere to its privacy policy, a deeper trust relationship is established-one that transcends ordinary private legal relations.

Fiduciary duties arise from imbalances in power, status, and information between stronger and weaker parties. [11] Given that platforms' control and regulatory authority over personal information, acquired through privacy policies, can no longer be adequately explained by contract theory alone, fiduciary duties provide a normative justification for platform self-regulation. [12] Moreover, they establish a set of protective mechanisms that account for power asymmetries between platforms and users. Duties of loyalty and diligence can guide platforms in avoiding the abuse of their dominant positions and ensure strict compliance with privacy commitments regarding personal data protection. A trust-based precondition helps mitigate the misuse of platform private power at its source, promoting the responsible and scientifically sound application of algorithmic technologies while strictly curbing misconduct.

5.1.2. Constructing an Endogenous Compliance System

Building an endogenous compliance system based on trust relationships can be approached through three dimensions: technological embedding, organizational transformation, and compliance responsiveness.

First, leveraging technology to establish a compliance framework. Platforms should adhere to the principle of data minimization by default when collecting users' personal information, gathering only what is strictly necessary for service provision to strengthen user trust. Basic and non-essential

functions should be differentiated, with a tiered consent model implemented-additional data collection should require explicit user activation. Sensitive personal information, such as ID numbers and facial data, should be automatically classified and encrypted using technical safeguards to eliminate exposure risks.

Second, fostering a shift toward collaborative organizational structures. Solely emphasizing platforms' unilateral control over users can degrade self-regulation. Instead, it is essential to open up platform private power and organizational architecture. Platform data compliance departments should incorporate user representatives in collaborative decision-making, making third-party assessments and evaluations a prerequisite for modifying privacy policies. External entities such as industry associations and data service providers, which more neutrally represent consumer interests, should serve as counterbalances to platform private power.

Third, instituting a compliance responsiveness mechanism. Privacy policies that promote trust relationships should not be drafted hastily and then shelved indefinitely. Given users' bounded rationality and collective action challenges, most cannot continuously monitor platform compliance with privacy policies. Thus, platforms must proactively disclose modifications to privacy policies, as well as regulatory and enforcement actions by government authorities. These compliance updates should be communicated through pop-up notifications or alerts, ensuring users can easily access and review them.

5.2. Empowering Users to Correct Power Asymmetries

The "recentralization" of cyberspace driven by platform private power exacerbates disparities in capability, status, and authority between platforms and users, while also undermining users' absolute control over their personal information as data subjects. Without empowering users, it is difficult to overcome the limitations of individual control and the collective coordination challenges faced by atomized users.

First, enhancing user participation in the democratic governance of privacy policies. If amendments to privacy policies materially affect user interests, opaque modification processes are insufficient to maintain trust. Even when changes are based on legal and regulatory updates-which often provide broad, high-level guidance-the translation of these requirements into specific policy terms leaves substantial room for deliberation. Platforms should provide avenues for user participation, incorporating feedback through dialogue with stakeholder representatives and selecting policy revisions that align with user interests. Concretely, platforms could: Integrate a feedback mechanism for privacy policy updates within the app interface. Assign dedicated personnel to address prominent concerns raised by users. Explicitly indicate in the finalized policy whether user input was incorporated.

Second, streamlining the exercise of user rights under privacy policies. While privacy policies are typically accessible as legal documents in an app's "Settings" section, the rights they grant often require navigating disparate app functions, hindering their utility as effective data management tools. To address this: Directly embed actionable rights interfaces (e.g., one-click "Delete Data" or "Export Data" buttons) within the privacy policy or settings. Provide timely customer support for technically complex requests.

Third, adopting user-friendly UI/UX design. Users lacking technical expertise or time are often overwhelmed by convoluted policy terms and multi-step workflows, leaving them no choice but to passively follow app prompts. Platforms should: Offer simplified, layperson-friendly summaries of privacy policies in easily accessible interfaces, highlighting only high-impact clauses. Use multimedia (e.g., videos, animations, infographics) to enhance comprehension. Retain the full policy version via hyperlink for optional review.

5.3. Government Regulation: Intervention and Its Limits

The degradation of self-regulatory mechanisms not only facilitates the abuse of platform private power but also structurally undermines the efficacy of public governance. When governmental regulation fails to adequately address societal demands, the consequent expansion of societal self-governance may progressively erode public trust and precipitate a crisis of legitimacy. [13] This is particularly evident in the realm of personal information protection, where the nominal "notice-and-consent" framework has been rendered largely symbolic. In this context, unmitigated self-regulation proves inadequate; instead, it is imperative to institutionalize embedded compliance mechanisms to establish effective governance.

Robust transparency mechanisms constitute a prerequisite for meaningful user understanding and participation in the democratic oversight of privacy policies. Data regulatory authorities can dynamically spot-check whether apps publicly disclose privacy rules in prominent positions. At the same time, the platform is required to keep the situation of soliciting and adopting opinions during the process of modifying the privacy policy for future inspection. It is also necessary to strictly review whether the privacy policy adheres to the principle of minimizing the scope of data collection. For terms with ambiguity, the platform should be required to provide further explanations.

Data regulatory authorities should also play a proactive role in the external oversight mechanisms of privacy policies. For instance, they could coordinate expert reviews to provide recommendations for privacy policies and promote the clarification and specificity of specific provisions. Additionally, they should foster the development of third-party certification markets to enhance the persuasiveness and credibility of privacy policy compliance. Furthermore, data regulators should recognize that in selecting regulatory methods and tools, administrative penalties should be used cautiously. They should respect the regulatory hierarchy that prioritizes self-regulation over government intervention and avoid excessively disrupting the spontaneous forces of the market. Soft regulatory measures, such as supervisory interviews, are conducive to guiding platforms in rectifying the negative effects of privacy policy misuse. The regulatory sandbox, as an innovative fault-tolerant mechanism, is particularly well-suited to the context of platform privacy policies. By establishing a safe space that allows technologies to enter the market while exempting them from legal liability for associated risks, it facilitates the organic integration of technological innovation and regulation.

6. CONCLUSION

The practical exploration in the field of personal information protection has demonstrated that the laissez-faire regulatory model, under which platforms gain information processing advantages through user consent in traditional privacy frameworks, is no longer mainstream. Privacy policies, as tools for platform self-regulation, leverage the initiative and flexibility of platforms themselves. However, with the enactment of the Personal Information Protection Law, embedding governmental compliance requirements into privacy policies to prevent the degradation of self-regulation has gradually become the prevailing regulatory approach. Neither self-regulation nor government regulation should be neglected.

For personal information to play a greater role, continuous technological advancements by platforms are necessary, but even more crucial is the evolution of regulatory models. In the context of platform governance, platforms act both as regulators and as entities subject to government oversight. Their architecture must accommodate user private rights, platform private power, and government public authority. The readability barriers and ambiguous clauses in privacy policies amplify platforms' data processing capabilities, while merely copying higher-level legal provisions in formalistic terms fails to address the granular requirements of personal information protection. Relying solely on platforms to meet personal information protection demands implies an expansion of their private power. Under the influence of such power, self-regulation may encroach upon the participation space of users and

the government, ultimately undermining its own effectiveness. While platforms' professional judgment is essential in addressing these issues, an open governance structure can encourage the public and data regulators to contribute broader perspectives on personal information protection.

Privacy policies should not be reduced to a one-sided tool for platforms to impose managerial order on users. Instead, they must serve as effective instruments for users to manage their personal information and assert their data compliance rights, ultimately fostering mutual trust among users, platforms, and the government.

REFERENCES

[1] Chengfeng Yu, “The Rise of Platform Media: Paradigms and Paradoxes of Privacy Protection”, Oriental Law, No. 5, pp. 75, 2024.

[2] Hanhua Zhou, “Parallel or Intersecting: The Relationship Between Personal Information Protection and Privacy Rights”, Peking University Law Journal, Vol. 33, No. 5:pp. 1169, 2021.

[3] Xinbao Zhang, “From Privacy to Personal Information: Rebalancing Interests in Theory and Institutions”, China Legal Science, No. 3, pp. 43, 2015.

[4] Huanxin Luo, “Privacy Policy's Past, Present, and Future: From Contract to Standard to Trust Endorsement”, Nanjing University Law Journal, No. 5, pp. 104, 2023.

[5] Yegang Wang, “Study on the Legal Effect of the Internet Privacy Policy: Centered on Personal information Protection”, Journal of Comparative Law, No, 1, pp 122, 2020.

[6] Bartle, I., & Vass, P, “Self-Regulation Within The Regulatory State: Towards A New Regulatory Paradigm?”, Public Administration, Vol.85, No.4, pp.888-890, 2007.

[7] Djumadi, Abdul Halim Barkatullah, “Does self-regulation provide legal protection and security to e-commerce consumers?”, Electronic Commerce Research and Applications. Vol. 30, July–August, p. 97, 2018.

[8] Song Jin, "Practice Review and Normative Approach of Mobile APP Privacy Policy", Tianjin Legal Science, No. 3, pp. 79, 2024.

[9] Huanxin Luo, “Privacy Policy's Past, Present, and Future: From Contract to Standard to Trust Endorsement”, Nanjing University Law Journal, No. 5, pp. 114, 2023.

[10] Jack M. Balkin, “Information Fiduciaries and the First Amendment”, UC Davis Law Review, Vol. 49, No. 4, pp. 1183, 2016.

[11] Jack M. Balkin, “The Fiduciary Model of Privacy”, Harvard Law Review Forum, Vol. 134, No. 1, pp. 26, 2020.

[12] Siqi Lu, “Application of Information Fiduciary Duty in Platform Organization Under the Theory of Meta-regulation”, Electronics Intellectual Property, No. 5, pp. 17, 2022.

[13] Mengyao Hu, “Theoretical Reflection and Paradigm Reconstruction of Social Self-regulation”, Law Review, No. 6, pp. 42, 2024.