International Journal of Law, Policy & Society

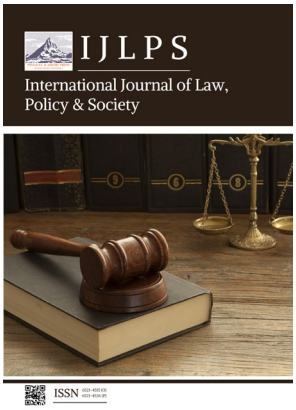
Vol. 1 No. 1 2025

Article **Open Access**

The Conflict Balance Model between Sovereignty and National Treatment in the Digital Age

Yuchen Han [1,*]

[1] The University of New South Wales, Sydney, New South Wales, Australia
* Correspondence: Yuchen Han, The University of New South Wales, Sydney, New South Wales, Australia



Received: 10 May 2025
Revised: 27 May 2025
Accepted: 09 June 2025
Published: 14 June 2025

Abstract: With the advent of the era of data sovereignty, the traditional principle of national treatment (NT) in international investment law faces significant challenges. Digital sovereignty emphasizes a state's absolute control over cross-border data flows and technical standards, prompting countries to impose trade barriers such as data localization and unfair digital taxes, which conflict with the principle of non-discrimination. This paper focuses on the dynamic balance between data sovereignty and national treatment, analyzing the root causes of their conflict, including the tension between sovereignty and open markets and the ambiguity of exception clauses. Measures strengthening digital sovereignty — such as fragmented technical standards and digital services taxes — exacerbate hidden discrimination against foreign investors, posing key dilemmas for the implementation of NT in the digital era. This study aims to explore institutional innovations that reconcile controllable market access with security interests, contributing to the reform of international investment law.

Keywords: data sovereignty; national treatment; digital taxation; international investment law

1. Introduction

The advent of the era of data sovereignty has restructured the global economic development order, and the principle of national treatment (NT) in traditional international investment law, that is, the host nation should grant foreign enterprises the same treatment as domestic companies, is facing a great challenge [1]. The reason is that digital sovereignty puts more emphasis on the absolute control of the state over the cross-border flow of data and technical standards, which reflects the serious exclusivity [2]. The global advancement of the digital currency economy increasingly relies on open and equitable markets. The two are bound to have policy conflicts: host countries often set up trade barriers such as data localization and unfair digital taxes, all of which may lead to potential deviations in national treatment; and investors' strong demand for free market access under the principle of "non-discrimination" also creates anxiety over sovereign intrusion. This contradiction reflects that the current international investment law is undergoing a transformation from "Investment Liberalization" to "Data Security Governance" [3,4].

This essay focuses on the dynamic balance between data security governance and national treatment in the era of digital sovereignty, and tries to answer two core questions: how to balance the demands of digital sovereignty and the effective realization of national treatment? What kind of institutional innovation does the principle of NT need to achieve adaptability in the context of the digital age? This research aims to transcend the tradi-

tional "zero-sum game" framework by exploring a balanced model that integrates "hierarchical data management" and "technical support", thereby contributing to the theoretical foundation for a reformed international investment system that accommodates both "controllable market access" and "security interests".

2. The Root Causes of the Contradiction between Data Sovereignty and National Treatment

The practical conflict between the framework of data sovereignty protection and the principle of NT in the original cross-border investment law is essentially the impact of national sovereignty governance and the opening of the global market in the digital age. The core contradictions can be summarized into two aspects. Both represent key obstacles to achieving the principle of national treatment in the digital era.

2.1. Sovereignty First or Open Markets

Digital sovereignty places greater emphasis on the state's absolute control over data, information, and technology. Its core lies in safeguarding national information security and public interests [5]. For instance, some countries' data protection frameworks, such as the cross-border data transmission review mechanisms established in their data security laws, regard data localization as a key expression of digital sovereignty [6]. Such policies encourage foreign investors to consider storing data within the host nation's territory or may mandate restrictions on cross-state data flows through technical standards, to ensure that the host country's government supervises key data [6]. However, in the principle of national treatment, the host state needs to treat foreign companies and native enterprises equally regarding access conditions and regulatory measures [1]. The legal basis for this is to better promote the free cross-border flow of capital to eliminate market barriers.

The conflicting demands of digital sovereignty and national treatment also reflect a fundamental opposition in policy goals. Take data localization as an example. To meet the data storage requirements of the host country, foreign investors need to establish additional local data centers. However, domestic enterprises, being located in the host country, can naturally avoid such costs. This disparity in compliance costs constitutes a deviation from the principle of national treatment, but host countries often justify it based on "data sovereignty security risks".

It is not difficult to see that the underlying contradiction lies in the host country's anxiety over sovereign intrusion. The globalization driven by the digital economy heavily depends on cross-border data flows and technological exchange. However, host nations inevitably harbor concerns that such openness may render their technologies vulnerable to foreign investors or lead to domestic sensitive information being compromised by external entities, thereby posing significant security risks. This pervasive anxiety has prompted countries to reinforce their sovereign boundaries through legislative measures. Take, for example, some countries' restrictions on certain foreign technology providers, which, though framed as national security measures, arguably reflect elements of digital protectionism. Although these actions are framed as "Security Protection", they arguably reflect elements of "Digital Protectionism". which stands in stark contrast to the non-discrimination principle inherent in national treatment.

2.2. The Equivocal Notion of Exception Clauses

International investment agreements typically include exceptional provisions related to national security and public policy, which, in principle, permit host countries to deviate from the implementation of national treatment under certain circumstances. However, due to the extremely ambiguous semantics of the exception clause, host countries often abuse the exemption mechanism.

It is evident from the expansion of the notion of "State Security" that host countries can readily integrate data supervision measures into their security frameworks. In 2020,

the United States, citing national security reasons, launched an investigation into TikTok and issued an executive order demanding a ban on its operations within the country, demanding a ban on its related business in the US [7]. In response, the company filed multiple lawsuits, arguing that there was no substantial security threat and that the ban could lead to unjustified economic loss, demonstrating that there was no substantial risk of economic losses to the defendant. Ultimately, a federal court issued a preliminary injunction to halt the enforcement of Trump's executive order.

From the perspective that "Public Policy" can be regarded as an exception, it has exacerbated the uncertainty of the provisions. Specifically, host countries may leverage this rationale to impose additional restrictions on the digital services provided by foreign investors, while local enterprises benefit from exemption treatments [8]. Such differentiated regulatory practices are challenging to accurately identify as discrimination in judicial proceedings and are likely to lead international arbitral tribunals into a dilemma regarding the "Legitimacy of Purpose" [8]. A prominent example is the European Union's Digital Markets Act (DMA), which imposes specific obligations on large technology companies through its "Gatekeeper" framework. Although these measures are not explicitly directed at foreign investors, they create potential for discriminatory treatment [9]. These also highlight the risk that exceptional provisions may be strategically applied by host countries, potentially turning into an instrument for digital protectionism. Fundamentally, these issues pertain to acquiring technological advantages through discriminatory regulations, which contravene the principle of national treatment.

Both of the aforementioned root causes of conflicts reflect existing institutional contradictions. In the context of traditional international investment, there is a tendency towards "Investment Freedom" to maximize returns, while in the era of digital sovereignty, "Risk Control" is given priority. The former relies more on the principle of NT to promote the liquidity of transnational capital, while the latter primarily reinforces the exclusivity of the digital domain through sovereign boundaries.

3. Key Dilemma to the Execution of National Treatment in the Digital Era

Strengthening digital sovereignty, while safeguarding national security, also has multiple impacts on the actualization of the principle of NT. The host country often restricts cross-border data flows and adopts differentiated regulatory models, which inevitably constitute an intangible "Digital Sovereignty Barrier" for foreign investors, resulting in a continuous impact on the utilization of the principle of NT in the data field.

3.1. Data Sovereignty Protection and the Fragmentation of Technical Standards

It is certain that the core of digital sovereignty lies in the control over data. Host countries often restrict the outflow of data through measures such as local data storage and cross-border transmission review [2]. Although these measures are justified on the grounds of national security, they often introduce institutional risks of indirect discrimination against foreign investors [2].

According to Article 36 of China's Data Security Law, the export of "Important Data" requires a security assessment. However, regulatory uncertainty and inconsistent interpretations of what constitutes "important data" create ambiguity, leading to unpredictable compliance risks for foreign enterprises, which inevitably leads to unpredictable compliance risks for foreign enterprises [6]. In 2021, Didi Chuxing was reviewed and taken down by the China Cybersecurity Review Office due to cross-border data flow issues. While the case did not directly involve discriminatory treatment against foreign shareholders, it nevertheless highlighted the potential threat of data sovereignty policies to foreign investors. Meanwhile, countries are differentiating to strengthen their national digital sovereignty by implementing technical standards, which also exacerbates market fragmentation on another level. An illustrative case is India's Digital Personal Data Protection Act, which stipulates that "Sensitive Data" must be processed locally, but the classification

standards lack transparency, which may pose challenges for foreign enterprises to make rational predictions [10]. Although none of these policies explicitly exclude foreign enterprises, their implementation will all lead to practical difficulties in the principle of national treatment.

3.2. Digital Tax Injustice and Hidden Discrimination Regulation

The Digital Services Tax (DST) can be regarded as a manifestation of the domain expansion of digital sovereignty. The design of its tax rate and the taxable objects all imply discriminatory tendencies towards foreign enterprises, triggering disputes over national treatment. Take the digital services tax in France in 2019 as an example. The tax rate was 3%, with "Digital Services Revenue" as the tax base. The tax targets were aimed at enterprises with worldwide earnings exceeding 750 million euros and French revenue exceeding 25 million euros. Although the tax targets seemed universal, more than two-thirds of the companies were from the United States. In particular, the tax disproportionately affected large U.S.-based technology companies such as Google and Amazon, raising concerns about its de facto discriminatory impact. However, from the perspective of national treatment, among the actual taxable objects, almost no French companies were affected, which also indicates that the policy is discriminatory in fact. In addition, it also includes the hidden regulatory discrimination brought about by the era of digital sovereignty. The Huawei v. FCC case in 2021 is a typical example. The FCC banned U.S. telecom operators from purchasing equipment from certain foreign suppliers, citing national security risks as justification. While the policy does not explicitly target foreign investors, its selective application may imply de facto differential treatment, in essence, under its continuous supervision, it emphasizes that Huawei constitutes a threat to the security of the US communication system [11]. From another perspective, this is a kind of differential treatment because domestic companies in the US do not pose the same risk. All these reflect that the "National Security Exception" is constantly expanding into an invisible barrier, eroding the realization of equal national treatment.

4. Balanced Approach

The commonality of the challenges outlined above underscores the predicament faced by sovereign states and foreign investors in the era of the digital economy. To achieve a dynamic balance between digital sovereignty and national treatment, it is necessary to avoid excessive market opening leading to the loss of cross-border data control. Concurrently, attention must be given to upholding the core principles of international investment law, particularly the principle of National Treatment (NT) [1]. Therefore, a dynamic linkage model of "Management + Technology" can be considered to be adopted to construct an innovative framework that takes into account both data sovereignty and market openness.

4.1. Data Grading Application

The essence of data classification is rooted in the implementation of differentiated governance. Based on the extent to which data impacts national security, public interests, and economic competitiveness, it is commonly classified into three hierarchical levels: core data, important data, and general data, which serve as the stepwise release of sovereign sensitive areas [6]. Core data refers to highly sensitive information related to national defense, military operations, and the overall functioning of the national economy. The cross-border flow of such data is prohibited, the authority of foreign-funded enterprises to access such data is restricted, a mandatory localized storage model is implemented, and and sovereign authority over such data is reinforced [6]. In contrast, important data about financial transactions and energy networks employs a "Negative List" mechanism that explicitly delineates sectors where foreign investment is restricted. Conditional cross-border

transfers are permitted but may be permitted, provided they undergo security assessments to ensure national compliance with risk management protocols. In addition, for the free flow of general data and information, such as consumer behavior data and publicly available commercial information, it is necessary to simultaneously meet the basic privacy protection standards through anonymization processing and other means, thereby thus enabling the application of national treatment through equal access and regulatory standards.

Hierarchical governance offers the advantage of a nuanced balance: The host country can ensure the bottom line of sovereignty by setting up a defense line for core data while simultaneously preserving the market competitiveness of foreign investors through the facilitation of general data flow. In India's Digital Personal Data Protection Act (2023), there is no separate classification for "Sensitive Personal Data"; however, it mandates adherence to guiding principles for data minimisation and purpose constraint [10]. This framework, to some extent, enables foreign investors to engage in cross-border data transmission under specified conditions, thereby mitigating the risk of trade retaliation that may arise from comprehensive regional lockdowns [10].

4.2. Linkage of Technology Applications

Essentially, the reduction of institutional frictions between security and openness can be facilitated through innovative digital technologies. Firstly, Quantum Key Distribution (QKD) can be employed to securely exchange encryption keys between transacting parties, thereby enabling data to remain usable yet invisible, preserving utility without compromising confidentiality [12]. Meanwhile, within the GAIA-X framework, a certain degree of data sharing can be attained by enhancing cross-border data traceability through the assignment of interoperable unique identifiers. This ensures that cross-border data flows can support more complex queries with verifiable integrity, thereby enhancing investor confidence and operational efficiency while improving overall data availability and assisting participants in their ability to search for relevant information [13]. The sensitivity associated with business-related data necessitates careful consideration of trust, security maintenance, and privacy preservation. The GAIA-X framework was specifically designed to address the twin challenges of data interoperability and privacy assurance, aiming to build an infrastructure that promotes equal data sharing simultaneously on the premise of risk reduction [13].

Secondly, the implementation of blockchain technology significantly enhances regulatory efficiency by automatically enforcing compliance terms by by replacing conventional agreements with self-executing smart contracts that automate compliance with regulatory standards [14]. Because of the nature of blockchain as a distributed digital ledger, it enables secure transaction recording without a third party, thereby reducing data exposure. All these can fundamentally alleviate the anxiety over the cost of manual review and enhance the transparency of regulation, thereby alleviating the concerns of foreign investors about "Hidden Discrimination" [14].

The interwoven application of hierarchical data governance and emerging technologies enables digital sovereignty to be both institutionally enforced through legal frameworks and operationally maintained through technological infrastructures. Such a model, on the one hand, can respond to the host country's concerns about "Security Risks", and on the other hand, it can compress the space for hidden discrimination through technological means.

5. Adaptive Transformation of the Principle of National Treatment

In the age of emerging big data, the concept of NT must transcend the "Formal Equality" characteristic of traditional cross-border investment law. It is essential to reconstruct both technological and regulatory frameworks to achieve a transformation that allows for the coexistence of "Substantive Equality" and "Controllable Risks". This transformation

requires simultaneous attention to three aspects: defense, refined standards, and dispute settlement, in response to the complexity of digital governance itself and the sensitivity of sovereign security systems.

5.1. Artificial Intelligence Risk Assessment

Implementing traditional national treatment often faces significant challenges and frequently depends on seeking post-event arbitration relief. Currently, it cannot adapt to the concealment and real-time nature of the digital supervision era. Artificial intelligence (AI) and big data technologies can construct a "Risk Prediction" model to identify and flag emerging risks in advance, thereby enabling a transition from reactive measures to proactive prevention and control strategies. Firstly, one can attempt to analyze the policy texts, judicial precedents, and enterprise behavioral data of the host country through machine learning to identify potential misconduct that exists [15]. In addition, Institutions such as the European Centre for International Political and Economic Affairs (ECIPE) have tracked global digital trade barriers by mapping policies and found that data localization, content restrictions, and measures involving foreign investment are all risk points that may trigger the invocation of national treatment provisions.

Most notably, the host country can pilot the regulatory sandbox model in collaboration with international organizations to test the risks of data flow, to ensure the smooth implementation of regulatory rules in this field in the future. Such a model can facilitate the testing of specific compliance procedures and help small and medium-sized enterprises avoid unnecessary burdens, thereby preventing disputes over national treatment.

5.2. Reconstruct the Criteria for "Similar Situation"

In traditional international investment treaties, the determination of "Similar Situations" is generally based on "Similar Products or Services" as the formal standard. However, in the context of the digital age, characterized by heightened sensitivity surrounding "Data Sovereignty", it is inevitable to introduce "Data Security Level + Necessary Supervision" as a dual measurement benchmark. This approach aims to respond to the controversy over the legality of the host nation's invocation of exceptional provisions typical of national security and public order.

5.2.1. Legitimacy Binding Hierarchical Data Application with Exceptional Provisions

Only 10% of the existing investment treaties contain general exception provisions, and most of them are limited to "Basic Security Interests" in emergencies [8]. In the digital age, the reason commonly used by host countries to invoke exception clauses is that data infringes upon national security [8]. However, the absence of objective determination standards raises concerns about potential abuse of these exceptions. By clarifying the scope of application for the exception provisions through the aforementioned balanced policy, namely "Data Hierarchical Application", this measure means setting differentiated national treatment obligations for different data risk levels. For example, Tesla has built a data processing centre in Shanghai in accordance with relevant local laws and policies, thereby implementing localized data storage and meeting regulatory compliance requirements. This stratification can significantly mitigate the risk of host countries excessively broadening the scope of the "Security Exception Clause", while reducing concerns that arbitration tribunals may misinterpret or overextend the limits of sovereign discretion due to the absence of objective criteria.

5.2.2. Transplantation and Application of the Original Experience of International Trade Law

Take Article 20 of the General Agreement on Tariffs and Trade (GATT) as an illustrative example, which permits member states to implement necessary measures under gen-

erally exceptional circumstances. Digital governance can still draw on these legal frameworks to help establish clearer criteria for identifying "data security exceptions". A primary consideration is the necessity of regulatory measures, which refers to a demonstrable and proportionate need to protect data sovereignty in specific contexts.

For example, the EU's Digital Markets Act (DMA) mandates certain gatekeeper obligations — such as data access and interoperability — designed to reduce the risk of excessive monopolies by enforcing fair platform access. Concurrently, the principle of proportionality remains essential in ensuring fair competition across the digital industry and preventing instances of discriminatory treatment from arising.

5.3. Establish a New Dispute Settlement Mechanism

In traditional dispute resolution, digital disputes often present significant challenges due to issues such as outdated rules and systems. Therefore, to address disputes involving crypto assets, digital contracts, and other matters related to emerging digital technologies, exploring technology-enabled arbitration models is essential. Since arbitration remains the most prevalent method for resolving commercial disputes, updating its rules to accommodate digital challenges can serve as a crucial breakthrough; thus, innovating digital dispute resolution rules can greatly enhance the effectiveness of this process [16]. The UK's Digital Dispute Resolution Rules allow arbitration to be evaluated simultaneously with experts, with flexible procedures that are targeted and professional [16].

In addition, a new type of digital copyright protection model, namely blockchain arbitration, has also been introduced in the international practice of digital dispute resolution. Its emergence serves as a complement to the arbitration database for technical dispute resolution and possesses several distinctive characteristics: these include the automatic suspension of execution facilitated by smart contracts, the selection modes of arbitrators that diverge from traditional arbitration practices, and the utilization of encoded evidence in place of conventional oral testimony, among others.

However, since this arbitration model has not been recognized worldwide, there are also certain legal controversies. Nevertheless, it is undeniable that this innovative development can function as a preferred mechanism for resolving disputes arising from smart contracts, as resolving such disputes requires relevant technical knowledge, such as blockchain technology, which precisely reflects that this dispute mechanism aligns with the technical specificity required for resolving such cases.

The adaptive transformation of the principle of NT in the digital era can seek breakthroughs in the form of a triple merger of the above-mentioned technological support, rule reconstruction, and dispute settlement, but its feasibility still faces multiple challenges. The most crucial point is that the expansive interpretation of digital sovereignty can easily lead to the "exception clause" becoming a perfect excuse for disguised protectionism. This explains why the "gatekeeper" obligations under the EU's Digital Markets Act have received mixed evaluations internationally, as some view them as necessary safeguards for digital sovereignty, while others regard them as potential tools for economic protectionism.

Furthermore, as a new dispute mechanism, blockchain arbitration has a promising future trend due to its alignment with technical characteristics. However, caution is still needed as its decentralized structure is essentially in conflict with traditional arbitration methods [16]. Therefore, only by adopting the idea of dialectical unity can we avoid falling into the practical trap of a blanket approach to technology and truly achieve a successful transformation in national treatment.

6. Conclusion

In the era of digital sovereignty, as the essential conflict between the absolute control of data security by various countries and the open market demands of foreign investors intensifies, the dilemma of sovereign states between the two has been highlighted. It also

indicates that the principles of traditional international investment law are facing challenges. With the realization of the principle of NT as the core of discussion, Under the traditional framework, national treatment relies more on the formal equality standard of "Equal Products or Services", but this reliance — when confronted with data localization and differentiated digital tax policies — often results in hidden discrimination, as well as ambiguous interpretations of exception clauses in investment treaties, which also often result in regulatory abuse of excuses. These problems have all created "Digital Sovereignty Barriers", eroding the substantive justice of the principle of NT.

To reconcile the above conflicts, this paper proposes a framework that combines "Hierarchical Data Management" and "Technical Support" to achieve a dynamic balance between sovereignty protection and open markets. By classifying data at different levels, differentiated governance that balances the two is achieved, aiming to ease concerns over sovereign data control among host states and alleviate investors' worries about hidden discrimination. Secondly, in the adaptive transformation of national treatment, it has been proposed to combine AI early warning with rule reconstruction, integrate sovereignty priority with international investment principles, and introduce new tools such as blockchain arbitration in dispute settlement. These measures aim to break through the "Zero-Sum Game" mindset and truly embark on a broad path from formal equality to substantive equality. While safeguarding data and operational security, while ensuring a controllable open market. Ultimately, it can not only guarantee digital sovereignty but also effectively achieve national treatment in the era of big data.

References

1. R. Dolzer, U. Kriebaum, and C. Schreuer, *Principles of International Investment Law*. Oxford: Oxford University Press, 2022. ISBN: 9780192857804.
2. Q. Zhang and A. Mitchell, "Data Localization and the National Treatment Obligation in International Investment Treaties," *World Trade Rev.*, vol. 21, no. 4, pp. 391–410, 2022, doi: 10.1017/S1474745621000549.
3. J. R. Markusen, *Trade versus Investment Liberalization*, 1997, doi: 10.3386/w6231.
4. L. Sun, H. Zhang, and C. Fang, "Data security governance in the era of big data: status, challenges, and prospects," *Data Sci. Manag.*, vol. 2, pp. 41–44, 2021, doi: 10.1016/j.dsm.2021.06.001.
5. S. Wood et al., "Digital Sovereignty: the overlap and conflict between states, enterprises and citizens," *Plum Consulting*, 2020.
6. Fa, Zhonghua Renmin Gongheguo Shuju Anquan (Data Security Law of the People's Republic of China), promulgated by the Standing Comm. Nat'l People's Cong., June 10, 2021.
7. D. Trump, "Executive Order 13942: Addressing the Threat Posed by TikTok, and Taking Additional Steps to Address the National Emergency with Respect to the Information and Communications Technology and Services Supply Chain," *Office of the Federal Register*, 2020.
8. J. Bonnitcha, L. N. S. Poulsen, and M. Waibel, *The Political Economy of the Investment Treaty Regime*. Oxford: Oxford University Press, 2017. ISBN: 9780198719540.
9. S. P. Hadebe, "Digital Sovereignty and Tight Regulation in the EU: Analysing the motivation behind the Digital Markets Act," 2022, doi: 10.2139/ssrn.4785054.
10. P. Naithani, "Analysis of India's Digital Personal Data Protection Act, 2023," *Int. J. Law Manag.*, ahead-of-print, 2024, doi: 10.1108/IJLMA-05-2024-0174.
11. Federal Communications Commission, "Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs; Huawei Designation; ZTE Designation," *Federal Register*, 2020.
12. M. Lazirko, "Quantum computing standards & accounting information systems," *arXiv preprint*, arXiv:2311.11925, 2023, doi: 10.48550/arXiv.2311.11925.
13. K. Mätäsniemi, "Solving Inter-Organizational Data Sharing Challenges with GAIA-X," 2023.
14. S. Mann, V. Potdar, R. S. Gajavilli, and A. Chandan, "Blockchain Technology for Supply Chain Traceability, Transparency and Data Provenance," in *Proc. 10th Int. Conf. Adv. Inf. Technol.*, New York, NY, USA: ACM, 2018, doi: 10.1145/3301403.3301408.
15. S. W. Bauguess, "The Role of Big Data, Machine Learning, and AI in Assessing Risks: A Regulatory Perspective," *SEC Keynote Address: OpRisk North America 2017*, Jun. 21, 2017.
16. E. P. Rusakova and E. E. Frolova, "Digital disputes in the new legal reality," *RUDN J. Law*, vol. 26, no. 3, pp. 695–704, 2022, doi: 10.22363/2313-2337-2022-26-3-695-704.