

Original Research Article

## A study on electronic evidence admissibility and allocation of burden of proof in data consumption disputes

Yu Zhou

*School of Law, Anhui University of Finance and Economics, Bengbu, Anhui, 233030, China*

**Abstract:** The growth of the digital economy has made algorithmic contracting the dominant mode of platform-based consumption, giving rise to frequent new types of disputes—Such as big-data price discrimination, algorithmic failures, and backend data tampering. In these disputes, the core original electronic data is unilaterally held by the platform, while consumers have access only to derivative evidence of considerably weaker probative force, creating a structural imbalance in the parties' evidentiary capabilities. The traditional civil-litigation rule of "he who asserts must prove" proves inadequate in digital consumption scenarios. Judicial practice suffers from vague standards for electronic data verification, inconsistent allocation of the burden of proof, ineffective enforcement of the obligation to produce documentary evidence, and a lack of technical fact-finding mechanisms. These problems lead to inconsistent adjudication in similar cases and severely hinder consumer remedies. Grounded in the fundamental theories of civil evidence law, this study proposes a comprehensive reform path: A layered and progressive burden-of-proof allocation system, refined binary admissibility standards for original and derivative data, strengthened platform obligations for document production and spoliation inference, and improved supporting mechanisms including technical investigators and expert assistants.

**Keywords:** data consumption; electronic evidence; burden of proof; digital economy

## 1. Introduction

The rapid expansion of the digital economy has fundamentally altered consumption patterns and transactional relationships. With the rise of platform economies, algorithm-based contracting has become the primary means by which consumers and businesses establish legal relations—Whether in online shopping, hotel booking, or ride-hailing services. Every consumer transaction is now converted into electronic data that can be recorded, stored, and analysed. At the same time, new types of consumer disputes—Big-data price discrimination, algorithmic failures, and backend data tampering—Are proliferating, posing serious challenges to the traditional evidence rules of civil procedure.

Electronic data was formally recognised as a statutory evidence type in the 2012 amendment to the Civil Procedure Law, and its evidentiary status has since been confirmed. However, data consumption disputes are distinctive in that all core transactional raw data resides on the platform's servers, under the platform's exclusive control. What consumers can typically produce in litigation are only screenshots, screen recordings, or other derivative evidence generated through manual intervention—Evidence whose probative force is far inferior to the original data held by the platform. This structural asymmetry in evidence distribution makes it difficult for the traditional "he who asserts must prove" rule to operate effectively in this context.

## 2. Dilemmas in admissibility and review of electronic evidence in data consumption disputes

### 2.1. Difficulties in reviewing the authenticity of electronic data

Assessing the authenticity of electronic data lies at the heart of evidence authentication. Yet in data consumption disputes, such review faces three interlocking difficulties.

First, technical barriers impede judicial review. Electronic data exists in binary code; its generation,

modification, and deletion can occur without leaving discernible traces. Without specialised technical knowledge, judges struggle to accurately evaluate the integrity and originality of the data—Especially on matters involving algorithmic logic and backend records, where conventional fact-finding methods prove inadequate.

Second, consumers' means of evidence collection are constrained. Consumers usually preserve evidence through screenshots or screen-recording, but such evidence is easily challenged as inauthentic. When consumers resort to non-standard collection methods, the resulting evidence often fails to meet the technical criteria required for electronic-data review. Notarisation may enhance probative value, but its cost imposes a significant financial burden on ordinary consumers.

Third, third-party preservation mechanisms are underdeveloped. Article 94 of the Provisions on Evidence in Civil Procedure provides that evidence provided or confirmed by a neutral third-party platform that records and preserves electronic data may be deemed authentic. In practice, however, the neutrality, technical reliability, and data-access convenience of such third-party platforms remain problematic. Consumers rarely preserve evidence through third-party platforms before a dispute arises, and after a dispute emerges, platforms are often unwilling to cooperate in providing original data—Rendering this mechanism largely ineffective.

## **2.2. The binary structure of original data and derivative data**

In data consumption disputes, electronic evidence can be divided into two tiers: original data and derivative data. Original data refers to first-hand information automatically generated, recorded, and stored by the platform system—including transaction logs, algorithmic pricing records, user-profile tags, and backend operation logs. Derivative data, by contrast, consists of evidence created by consumers through screenshots, screen-recording, or photography, which reproduce or transform the original data. Original data, controlled by the platform, enjoys relatively high authenticity and completeness but is largely inaccessible to consumers. Derivative data, while in consumers' hands, suffers from inherent weaknesses: It may omit critical information due to improper capture, or fail to fully reflect the original data owing to technical limitations.

## **3. Structural imbalance in the allocation of burden of proof**

### **3.1. The applicability dilemma of the "he who asserts must prove" principle**

The Civil Procedure Law establishes the basic rule that "he who asserts must prove." In traditional consumer disputes, this principle generally maintains a rough balance of evidentiary capabilities between the parties. But in data consumption disputes, owing to the structural asymmetry of evidence distribution, its application produces serious distortions.

To succeed in a claim of big-data price discrimination, a consumer would need to prove: (i) that the platform offered different prices to different consumers; (ii) that the price differentials were based on the consumers' personal information or consumption habits; and (iii) that the platform acted with subjective fault. Yet all key evidence—Pricing algorithms, user tags, historical transaction data—Is stored exclusively on the platform's servers, beyond the consumer's reach. In this situation of "evidence asymmetry," applying the "he who asserts must prove" rule effectively shifts the entire risk of non-persuasion onto the consumer.

### **3.2. Institutional possibilities and limits of reversing the burden of proof**

In response to this dilemma, both scholars and practitioners have shown interest in reversing the burden of proof. Some argue that in big-data price-discrimination cases, once consumers provide preliminary evidence suggesting possible discrimination, the burden should shift to the platform to prove the lawfulness and reasonableness of its pricing practices. As the actual data controller and algorithm designer/operator, the platform has the technical capacity and data access to demonstrate its own compliance—Capabilities that consumers entirely lack.

However, reversing the burden of proof faces clear institutional obstacles under current law. First, such reversal requires explicit statutory authorisation, and no existing law specifically provides for it in data consumption disputes. Second, even if reversal were applicable, the operative standards—Such as the platform's burden to "prove absence of fault," the types of evidence acceptable, and the grounds for exoneration—Lack clear operational criteria, making effective implementation difficult in practice.

### 3.3. The hollowing-out of the obligation to produce documentary evidence and the absence of spoliation inference

The Provisions on Evidence in Civil Procedure extend the "order to produce documentary evidence" to audio-visual materials and electronic data. This mechanism was designed to be a powerful tool for overcoming evidentiary hurdles in data consumption disputes, but in practice it has largely been hollowed out.

First, the threshold for applying for such an order is high. The applicant must specify the name or content of the requested evidence, the facts to be proved and their materiality, and the basis for believing the opposing party controls the evidence. In data consumption disputes, consumers often cannot even accurately describe the name or content of the evidence, let alone satisfy these conditions. Second, the mechanism lacks effective sanctions. Although the rules allow the court to deem the asserted facts established if the opposing party unjustifiably refuses to produce the evidence, courts have been hesitant to apply this inference. Platforms frequently refuse production on grounds of "trade secrets" or "technical secrets," and judicial scrutiny of such defences is inconsistent. Third, the scope for spoliation inference is limited. Technical operations such as backend-data modification or deletion are difficult for consumers to detect and prove, making it hard to trigger the prerequisites for spoliation inference.

## 4. Paths for institutional improvement

### 4.1. Establishing a layered and progressive burden-of-proof allocation system

The core solution lies in constructing a burden-of-proof allocation system tailored to the characteristics of data consumption disputes. This study proposes a three-tier progressive framework: Preliminary burden → shift of burden → reversal of burden.

First tier – consumer's preliminary burden: The consumer must adduce preliminary evidence sufficient to show a possibility of the alleged infringing conduct. In big-data price-discrimination cases, this could include screenshots showing price differences for the same product/service when queried from different devices or accounts, or evidence that the platform's advertised promotional commitments are inconsistent with actual prices. The standard for this preliminary burden should be lower than "preponderance of the evidence"—Only "reasonable suspicion" or "prima facie" proof is required. Some scholars suggest that in personal-information leakage cases, once the consumer proves a high probability of leakage, the burden should shift to the platform.

Second tier – shift of burden: Once the consumer meets the preliminary burden, the burden shifts to the platform. The platform must submit original data—Pricing algorithms, user tags, transaction records—To demonstrate the lawfulness of its conduct. This shift is justified because the platform, as the actual data controller and algorithm operator, has clear informational and technical advantages in proving its own compliance.

Third tier – reversal of burden in specific circumstances: In cases involving algorithmic black boxes, system failures, or other technically complex matters where consumers are entirely unable to obtain evidence, the burden should be reversed outright—Requiring the platform to bear the full burden of proving its absence of fault. This is not a wholesale rejection of "he who asserts must prove," but rather a targeted correction of the structural imbalance in evidentiary capabilities under specific scenarios.

### 4.2. Refining binary admissibility standards for original and derivative data

Given the binary structure of original and derivative data, differentiated admissibility standards should be adopted.

For original data: The platform should, in principle, produce the original storage medium or technically verified copies. As the data controller, the platform is obliged to submit complete, unaltered original data in litigation. If the platform invokes trade secrets, it may apply for protective measures (e.g., in-camera review), but may not refuse production solely on that ground.

For derivative data: The threshold for admissibility should be appropriately lowered. Evidence fixed by consumers via screenshots or screen-recordings, so long as it forms a coherent chain of proof and corroborates with other evidence, may be accepted as a basis for fact-finding. Where the consumer genuinely cannot obtain the original data, the probative value should not be denied merely because of formal deficiencies in the derivative evidence.

For third-party preserved data: Its evidentiary effect should be further clarified through judicial guidelines.

#### **4.3. Strengthening the platform's obligation to produce documentary evidence and spoliation inference**

To counter the hollowing-out of the document-production obligation, the following improvements are proposed:

(1) Lower the application threshold for orders to produce documentary evidence. In data consumption disputes, consumers often cannot precisely specify the evidence's name or content. They should be permitted to apply by describing the type and function of the evidence, without being required to name it exactly.

(2) Clarify the adverse consequences of unjustified refusal. Where a platform refuses to produce electronic data without proper justification, the court should make an adverse factual inference against it. The standards for reviewing "trade secret" or "technical secret" defences should be unified to prevent abuse.

(3) Establish industry norms for the preservation and disclosure of electronic data.

#### **4.4. Improving supporting mechanisms for technical investigators and expert assistants**

Given the lack of technical fact-finding mechanisms, the technical-investigator system used in intellectual property adjudication should be extended, *mutatis mutandis*, to data consumption disputes.

Technical investigators may be appointed to participate in proceedings. Their duties should include: Clarifying the technical issues in dispute, advising on the scope and methods of technical investigation, and providing professional opinions on matters such as electronic-data integrity and authenticity.

Expert assistants should have clearer rules on selection, rights, duties, and liability. They may opine on algorithmic logic, data-generation processes, system-failure causes, etc. Mechanisms should also be established to safeguard their neutrality, preventing them from becoming mere "hired witnesses" for a party.

Judicial appraisal for electronic data should be supported by specialised institutions and technical standards. Electronic-data appraisal involves data recovery, algorithm verification, system auditing, and other specialised fields, requiring qualified institutions and personnel. National technical standards and industry norms for electronic-data judicial appraisal should be promoted.

### **5. Conclusion**

In data consumption disputes, key electronic evidence is unilaterally monopolised by platforms, consumers' evidentiary capacity is severely inadequate, and the traditional "he who asserts must prove" rule fails to deliver substantive fairness. Judicial practice is plagued by vague review standards, inconsistent allocation rules, and the absence of supporting mechanisms, leading to divergent outcomes in similar cases. To resolve this predicament, we must establish a layered and progressive burden-of-proof allocation system, refine binary admissibility standards for original and derivative data, strengthen the platform's production obligations and spoliation inference rules, and improve supporting mechanisms such as technical investigators. These reforms aim to correct the procedural imbalance between the parties, unify adjudicative standards, and solidify the rule-of-law foundation for the digital economy.

### **References**

- [1] J. Xie: Judicial Protection of Data Property Rights and Interests in Live Streaming, *Journal of Shandong University of Science and Technology (Social Science Edition)*, Vol. 27 (2025) No. 4.
- [2] Allocation of Burden of Proof in Online Shopping Litigation, *Legal Expo*, Vol. 23 (2023) No. 23, p.31-33.
- [3] P. Wang: Methods for Authenticating the Authenticity of Electronic Data, *Civil Justice*, Vol. 3 (2020) No. 3, p.46.
- [4] From the "First Big Data Price Discrimination Case" to the Risks and Protection of Consumer Rights in the Digital Economy, February 24, 2025. (EB/OL).
- [5] An Analysis of the Application of the Principle of Reversal of Burden of Proof for Electronic Data Evidence, *Legal System and Society*, Vol. 8 (2021) No. 8.
- [6] P.X. Liu: Legal Positioning and Evidence Rules of Electronic Evidence (forthcoming/incomplete). Notes on Reference Formats (for the journal's style).