# The Legal Protection of Personal Financial Information Rights: A Core Analysis of Data Ownership and Utilization Rules

**Zhao Xinyu**
*Belarusian State Economic University, Minsk, Republic of Belarus*

**Abstract: FinTech innovation has caused an unprecedented proliferation and commodification of PFI as the financial industry quickly goes digital. While this change is great for convenience and being able to access things, it leaves people at a serious risk of data breaches, getting discriminated against based on their profile, and losing privacy. The article discusses the important legal problem of safeguarding PFI rights by concentrating on these two major parts：conceputation of ownship of data and creation of solid utilization rules. We argue an old-fashioned, property-based notion of ownership simply cannot properly accommodate the nonrivalrous and co-created qualities of PFI. rather than a framework focused on a "rights bundle" for individuals (rights of access, portability, etc.)and the imposition of a "data stewardship" or "fiduciary duty" on financial institutions. The paper assesses the shortcomings of consent - centric mechanism & pushes for greater focus on ex ante control s like Purpose limitation & Data minimization. By way of comparison between these emerging regulatory principles, it is argued that any successful sustainable protection of PFI must shift from reliance on an elusive notion of consumer consent to a set of concrete obligations for the controller of personal information that can be enforced to balance the needs for financial innovation against a fundamental right to privacy.**

**Keywords: Personal Financial Information (PFI); Data Protection; Data Ownership; Data Utilization Rules; Privacy Law; FinTech Regulation; Data Stewardship**

## 1. Introduction

The world's financial situation is experiencing a huge change. This is being caused by digital technology. FinTech, mobile banking, algorithmic trading and all of them are changing the way people deal with money, and this is thanks to a very valuable thing called data. Personal financial information (PFI) is blood of this new ecosystem, it make all personalized services and complex risks modeling possible[1]. But this view of the world as data means big things for us as individuals. A huge amount of detailed data sets produce a very detailed picture of a person's life. The danger of being wronged through data breaches, unclear algorithmic choices causing financial exclusion, or having personal data used without consent can directly harm our sense of freedom and money situation[2]. Legal frameworks from the analogue time, it's having trouble catching up with these new digital realities.

This article argues that any solid legal regime around PFI rights must rethink two main ideas: who owns the data and what data usage rules apply. The murky question as to who "owns" financial data is a major legal dispute which governs the balance of power[3]. We claim that it is simple property is not enough. More refined "bundle-of-rights," which acknowledges individual control rights together with institutional stewardship obligations. At the same time, the rules for collecting, handling, and sharing data must be strict and enforceable This paper shows that the dominant legal fiction "notice and consent" has failed and that we need new substantive limitations such as purpose limitation and data minimization. Next we will do our analysis by defining what is special about PFI's scope, analyzing "ownership puzzle" and giving the necessary rules of utilization before finishing off with a unified vision of a protect laws.

## 2. The Unique Sensitivity and Scope of Personal Financial Information

Defining an object of protection is necessary. PFI is very different from others as it is highly sensitive and comprehensive and thus needs a higher threshold from the perspective of law than normal people[4]. It's not a single thing, but

 

a whole spectrum of data points giving us a look behind the curtain at what it's like to be them. Namely accounts, SSNs - static identifiers – purchases, payments, location – dynamic, financial transactions, loans, credit score – economic opportunity through credit data, the front door – Most importantly, much of modern PFI includes data derived by inference and behavior – profiles, spending patterns, risk analysis, etc – which are often obscure but powerful. It is sensitive because it involves life and death directly, it involves the economic survival of a company, any mistake can mean heavy financial losses, identity theft, reputation loss[5]. Financial data is also by nature longitudinal, resulting in an unerasable record that can be used to either include or reject an individual. Here is Table 1, which classifies this data.

**Table 1. Classification of Personal Financial Information (PFI)**

| Category | Description | Examples | Primary Risk |
|---|---|---|---|
| Identity & Account Data | Information used to identify an individual and access their financial accounts. | Full Name, Address, Social Security Number (SSN) / National ID, Bank Account Number, Credit Card Number, Passwords, Biometric data. | Identity Theft, Fraud, Unauthorized Access. |
| Transactional Data | A record of an individual's financial activities, movements, and behaviors. | Purchase history, Payment records, Money transfers, ATM withdrawals, Geolocation data from payments, Investment records. | Profiling, Surveillance, Behavioral Manipulation, Revelation of personal beliefs or associations. |
| Credit & Solvency Data | Information pertaining to an individual's creditworthiness and financial standing. | Credit reports, Credit scores, Loan applications, Debt history, Income records, Bankruptcy filings. | Financial Exclusion, Discriminatory Lending, Errors in assessment. |
| Inferred & Profiled Data | Data created by financial institutions through analysis of other PFI. | Spending habit profiles, "Risk" or "Customer Value" scores, Algorithmic financial advice, Predicted future earnings, Inferred financial goals. | Algorithmic Bias, Lack of Transparency ("Black Box"), Unfair treatment. |

PFI's overall damage, which can be seen in Table 1, is displayed: One transaction could hint at your private personal tieups or state of health: Aggregate transactional data after machine learning processing will enable institutions to predict with likely discriminatory and unquestionable models. Taking a low-income neighborhood that has the pattern which is linked to a higher credit risk like an algorithms instance, that would continue to perpetuate this systemic financial exclusion. Therefore, the law has to view PFI as a substitute of a person's life and chances[6]. It needs a legal frame that goes over simple fraud prevention to tackle the big dangers created by watching, sorting, and the unfair biases in today's money system. Protect them all, for the pficategorizing from call to delete.

## 3. Deconstructing the "Ownership" of Personal Financial Information

One of the key debates in data protection legislation is 'ownership'. This is also a significant issue for PFI, is does the data 'belong' to the individual or to the institution? To this (quán shǔ) question, there can be an answer that is foundational, which will dictate the allocation of rights. If the individual "owns" it, then they've got very strong, property-based control. if this institution "owns" it, then I am just data, with very few statutory rights[7]. However, applying traditional property concepts to an intangible, non-rivalrous, and co-created asset like data is fraught with difficulty. Data is jointly held by numerous parties at once, and a transaction is "co-created." Thinking about data as plain property isn't practical because it might interrupt vital information flows for credit reporting or fraud protection.

Due to the restrictions of the property model, academics have turned toward other paradigms. More productively, it moves away from the simple binary "own" question, to one which looks at "a bundle of rights," like the EU's GDPR. It doesn't grant complete "ownership" but rather gives the individual certain, enforceable, rights: access, correct, erase and move[8]. This decouples control from ownership. At the same time, this model also places a 'data stewardship' - a fiduciary duty - on financial

 

institutions which obliges them by law to act in the best interests of the data subject using a standard of care, loyalty, and confidentiality. The superior model acknowledges the practical need for data processing but frames it as a kind of privilege that is conditional, not an ownership right. The comparison is in table 2.

**Table 2. Comparative Models of Data "Ownership" and Control**

| Model | Core Concept | Rightsholder(s) | Implications for PFI Protection | Limitations |
|---|---|---|---|---|
| Data as Property | Data is an asset that can be owned, bought, and sold, like real estate. | Primarily the Individual (as creator) or the Institution (as collector). | Strong, exclusive rights for the "owner" to control use and alienation. Potentially enables data markets. | Data is non-rivalrous and co-created. Impractical to manage. Risks commodification of privacy. |
| Data as Privacy Right | Data is an extension of the person; control over it is a fundamental human right. | The Individual (Data Subject). | Protection is an inalienable right, not a tradable commodity. Focus on preventing harm and ensuring dignity. | Can be abstract. May conflict with economic goals and free flow of information (e.S., for credit). |
| Data as a "Bundle of Rights" (Stewardship Model) | Data is not "owned." The individual has specific control rights (access, portability, etc.), and the institution has a fiduciary duty to act as a steward. | Individual (Control Rights) & Institution (Use Rights & Fiduciary Duties). | Balances individual control with practical needs of commerce. Imposes high standard of care on institutions. | Requires complex regulation and strong enforcement to define and police fiduciary duties. |
| Data as a Public Good | Data, particularly in aggregate, is a social resource that should be accessible for public benefit (e.g., research, economic planning). | The Public / The State. | Prioritizes societal benefits over individual or corporate control. May involve mandatory data pooling. | Grave risks to individual privacy and autonomy. Potential for state surveillance and misuse. |

From Table 2 we see that the most pragmatic would be the “Bundle of Rights” or the stewardship model. It doesn't end up in a dead-end with the property model, where it's either a locked-down data or a “pay-for-privacy” nightmare It fortifies the abstract concept of a “privacy right” through real, actionable rights (e.g., portable information) and imposing binding, high-stakes fiduciary obligations on financial firms. By moving the legal focus from “who owns what data?” to “what are the institution’s responsibilities as a data steward?” and “what specific control does the person have?” this model would align the law with digital-economy realities, which creates a good, ethical base for PFI.

## 4. Crafting Utilization Rules I: The Failure of Consent and the Rise of Substantive Limits

even with “ownership” sorted out, the essence of protecting data is about the (lì yòng guī zé) or utilization rules. Historically this was on an individual opt in. The "note and consent" mode considers processing legitimate if an individual clicks "I agree" to a long and unreadable policy. For pfi, this model is a total failure. There is a huge power imbalance between institutions and users; the “power” to receive opaque or reject essential services is merely an illusion. “Consent fatigue” and the complexity of modern data flows, where “data” is bundled, shared, and re-purposed, means the consent-based construction is merely a legal fiction which indemnifies rather than empowers the institution.

Given the insufficiency of consent, a modern legal regime has to shift from after-the-fact to ex-ante substantive limitation on data collection irrespective of consent. The two most powerful principles are those of Purpose limitation and Data minimization. The purpose-limitation requires that PFI is only collected for one particular, certain reason and cannot be processed for purposes other than those for which it was originally used[9]. For example, just because a bank has your data for a wire

 

transfer doesn't mean it can then use it for marketing. That would add a brake on “function creep.” Data minimization is the idea that an institution should gather only the minimum PFI it needs for the exact reason it said it needed the data. It challenges the idea that we should be gathering it all. An instance would be an institution not collecting individual grainy spending behaviors for a loan requirement if a credit score and income verification can do. These principles make it such that they need to justify what they're doing with the data rather than you having to justify why you don't want them to do it. Table 3 Draws A Contrast:

**Table 3. Primary Legal Bases for Processing Personal Financial Information**

| Legal Basis | Description | Example in Finance | Risk of Misuse |
|---|---|---|---|
| Consent | The individual has given clear, unambiguous, and informed permission for a specific processing activity. | "Do you agree to receive our weekly marketing newsletter?" | High. Consent is often bundled, coerced, or not truly informed. "Consent fatigue" is rampant. |
| Performance of a Contract | Processing is necessary to fulfill a contract with the individual. | A bank processing a loan application or executing a requested stock trade. | Low-to-Medium. The "necessity" can be interpreted overly broadly ("function creep"). |
| Legal Obligation | Processing is necessary for the institution to comply with the law. | Anti-Money Laundering (AML) and Know Your Customer (KYC) checks required by statute. | Low. The purpose is clearly defined by external law, though data retention rules must be strict. |
| Legitimate Interest | Processing is necessary for the "legitimate interests" of the institution, unless overridden by the individual's rights. | Using transactional data for internal fraud detection models. | Very High. This is a flexible, balancing-test-based ground that institutions often use as a catch-all justification for activities like profiling or marketing. |
| Protection of Vital Interests | Processing is necessary to protect someone's life. | Rare in finance. E.g., disclosing data to emergency services if a transaction suggests immediate physical harm. | Very Low. |

From Table 3, we can see that consent is merely one option, and the most problematic. Contractual necessity and legal obligations are clear, but “legitimate interest” is too flexible and is easily abused. PFI will be sensitive, with strong frameworks, a robust PFI must greatly reduce “legitimate interest” justification for sensitive PFI – perhaps an impact evaluation would be required. Secondly, it should place greater emphasis on making purpose limitation and data minimization general rules for all legal bases. Even when processing for a “legal obligation” like KYC, data minimization still applies and only the minimum amount of data must be collected to comply with the law. Putting more emphasis on real “purpose” and “necessity” instead of fake "consent", that’s how we could properly protect people.

## 5. Crafting Utilization Rules II: Governing Algorithmic Profiling, Sharing, and Security

Utilization rules have to go through the whole data life, including algorithms, other entities and safety. Automated decision and profiling is finance, the algorithm makes decisions on mortgages, credit limits, and customer service. These systems are quick and efficient but cause “black box” opacity and algorithmic bias. A model using old data would find better ways to ‘red-line’ whole communities, continuing the bias. So it is critical that a utilization rule must be the right to an explanation, and the right to have a human review any significantly solely automated decision[10]. People need to be able to go up against an algorithmic refusal of credit and have it scrutinized by someone who knows about the big factors at play. To have such a check on the power of an algorithm is to have a fair and just society.

Utilization rules should apply for pfi sharing too. The financial ecosystem is like a tangled web of banks, credit bureaus, and FinTech apps. "Open Banking" tries to share data with APIs, but that makes it easier for bad guys to break in and invade your privacy. The law has to hold someone strictly accountable for the “data tail.” The original institution (data steward) had better be accountable for how the data is used by its

 

partners. It calls for strong data-sharing agreements and strict technical standards, all being open A person should see all data sharing from one screen, from Table 4. lastly, security is also an unarguable usage rule. And the duty to protect PFI from breach is a bedrock element of the stewardship duty, and it is a binding legal duty in the sense that it is more than just an exercise in form.

**Table 4. Key Regulatory Principles and Rules for PFI Utilization**

| Principle / Rule | Objective | Key Regulatory Actions |
|---|---|---|
| Purpose Limitation | To prevent "function creep" and ensure data is used only for the specific reason it was collected. | Require explicit, specific purposes to be declared at collection. Prohibit repurposing of data without a new, distinct legal basis. |
| Data Minimization | To reduce risk and irrelevance by limiting collection to what is strictly necessary. | Mandate that only the minimum data required for the specific purpose be collected. Enforce "privacy by default." |
| Accountability & Stewardship | To assign clear responsibility for the protection and ethical use of data. | Designate a data controller with fiduciary-like duties. Require Data Protection Impact Assessments (DPIAs) for high-risk processing. |
| Transparency | To ensure individuals know what data is held and how it is used. | Mandate clear, layered privacy notices. Provide individuals with a dashboard to see their data and its uses/sharing. |
| Rights in Automated Decision-Making | To combat algorithmic bias and "black box" opacity. | Grant the "right to an explanation" for automated decisions. Guarantee the right to a human review of significant decisions (e.g., loan denial). |
| Data Security & Breach Notification | To protect data integrity and confidentiality and to manage breaches. | Mandate "security by design." Enforce strong encryption, access controls, and auditing. Require prompt, clear notification to individuals and regulators after a breach. |
| Data Portability | To empower individuals and promote competition. | Grant individuals the right to receive their data in a structured, machine-readable format to transfer to another service provider. |

The principles in Table 4 form a comprehensive set of governance principles on how to deal with PFI use, going more than one-off consent. Data portability (Row 7) is a formidable tool, both an individual right and a pro-competitive measure which can break down “data silos.” The “right to an explanation” (Row 5) directly responds to 21st Century Algorithmic issues. But in the end, these utilization rules are where the abstract becomes real. Without something real to enforce, “ownership” is just an idea. By adding a stewardship model (Section 3) to these strong utilization rules (Sections 4 and 5), the conditions have been created for the legal framework required by the digital financial age.

## 6. Conclusion

This article presented a legal framework for the protection of PFI by focusing mainly on the aspects of the data owner and his uses. Digitalization of finance brings opportunities but can result in systemic risks to privacy. We stated that old legal constructs aren’t adequate. "Data ownership", rooted in property law, isn’t suitable for PFI. A better model would discard the binary “do I own it” question and favor a “bundle of rights” for individuals (access, portability) with a legally binding “data stewardship” or fiduciary responsibility for financial institutions. This rephrases it as a trusted keeper rather than an owner. At the same time, we showed the failure of 'notice and consent' because of power imbalances. PFI protection’s heart needs to be solid; it’s about using pre-existing data properly: limiting the purposes and minimizing the use. We limit excessive collections with strong data protection. This framework also has to include some of the more modern ones, like right to explanation with regard to algorithmic decision making and very strict accountability when it comes to data sharing. Financial law’s future is all about data law. Balancing new things’ innovation and basic rights is the main regulatory issue. It will be a legal system based on data stewardship and substantive utilization rules—not the fictions of property and consent—that is the only sustainable path forward.

 

**References**

[1]Zhang Y T. On the Legal Protection of Financial Consumers' Personal Information in the Context of Big Data[D]. Qinghai Normal University, 2025. https://doi.org/10.27778/d.cnki.gqhzy.2025.000112.

[2]Fang L, Li W Q. Improvement of Financial Data Sharing Rules from the Perspective of Personal Financial Information Protection[J]. Financial Law Review, 2021, (03): 79-88.

[3]Li A. Review of the Personal Control Model in Personal Financial Information Protection——A Study on Personal Financial Information Protection Based on Judicial Big Data[J]. CUPL Legal Review, 2024, 40(02): 23-35.

[4]Yang T S. Research on the Legal Regulation of Personal Financial Information Processing in the Big Data Era[D]. Lanzhou University of Finance and Economics, 2025. https://doi.org/10.27732/d.cnki.gnzsx.2025.000482.

[5]Liu S. Research on Legal Issues of Personal Financial Information Protection[D]. Jilin University of Finance and Economics, 2024.

[6]Zhang Y S. Research on the Informed Consent Rule in Personal Financial Information Protection[D]. Inner Mongolia University of Science and Technology, 2025. https://doi.org/10.27724/d.cnki.gnmgk.2025.000155.

[7]Lu X. Research on Legal Issues of Fintech Supervision[D]. Hebei University, 2023. https://doi.org/10.27103/d.cnki.ghebu.2023.002960.

[8]Cao P, Luo X P. Dilemmas and Improvement Countermeasures of the Legal Protection of Personal Financial Information in the Perspective of Digital Economy[J]. Journal of Shaanxi University of Technology (Social Sciences Edition), 2024, 42(02): 1-8+32.

[9]Ruan S K. Theoretical Clarification and Legal Realization of the Security Guarantee Obligation in the Sharing of Personal Financial Data[J/OL]. Journal of Northeastern University (Social Sciences Edition), 1-10 [2025-11-07]. https://doi.org/10.15936/j.cnki.1008-3758.2025.06.010.

[10]Li J. Discussion on Risk Control Strategies of Enterprise Financial Sharing from the Perspective of Big Data[J]. Journal of Shanxi University of Finance and Economics, 2025, 47(S2): 168-170.

 