# Business Value of Privacy-Preserving Mobility Analytics in Platform Operations: A Federated Risk-Utility Framework

Eren Demir[1], Selin Arslan[2], Murat Kaya[3,*]

[1]Department of Management Information Systems, Sakarya University, Sakarya 54050, Turkey

[2]Department of Business Administration, Bandirma Onyedi Eylul University, Balikesir 10200, Turkey

[3]Department of Industrial Engineering, Karabuk University, Karabuk 78050, Turkey

*Email: murat.kaya@karabuk.edu.tr (Corresponding Author)

## Abstract

Mobility platforms depend on continuous analytics of location traces, travel time, pickup density, delivery reliability, and user behavior. These data create operational value, but they also expose platforms to privacy, regulatory, communication, and trust risks when raw trajectories are centralized. This article develops a federated risk-utility framework for evaluating the business value of privacy-preserving mobility analytics in platform operations. The framework compares five analytics architectures: centralized raw-data analytics, local-only analytics, basic federated learning, differentially private federated learning, and a governed federated design that combines privacy controls, secure aggregation, compression, and managerial value gates. A numerical scenario analysis is used to examine prediction utility, privacy exposure, communication cost, expected regulatory loss, customer trust, and risk-adjusted operating value across ride-hailing, delivery, courier, and shared-mobility settings. Results show that the highest predictive utility does not necessarily create the highest business value. The governed federated risk-utility architecture produces the strongest risk-adjusted operating value because it preserves most of the operational benefit of mobility analytics while substantially reducing privacy exposure and compliance loss. The study contributes a business analytics perspective on federated mobility intelligence and provides actionable governance thresholds for platform managers.

**Keywords:** Mobility analytics; platform operations; federated learning; privacy preserving analytics; risk utility framework; business value; urban trajectory mining; data governance

**Article History:**

**Received:** January 23, 2025

**Revised:** March 18, 2025

**Accepted:** May 21, 2025

**Available Online:** June 30, 2025

 https://doi.org/10.63646/jbda.2025.030204

# Business Value of Privacy-Preserving Mobility Analytics in Platform Operations: A Federated Risk-Utility Framework

## 1. Introduction

Mobility platforms have become central coordinators of urban transportation, local commerce, last-mile logistics, and service work. Their operating models depend on the continuous interpretation of location traces, travel times, driver availability, merchant demand, pickup failures, and delivery delays. A platform that can accurately anticipate where demand will emerge, how long a route will take, and which worker or vehicle should be matched to a request can reduce waiting time, improve asset utilization, and protect service-level agreements. Yet the same data that generate operating value also reveal highly sensitive behavioral patterns. A sequence of GPS points can disclose a customer's home, workplace, medical visits, religious activities, social relationships, or working schedule. This tension makes mobility analytics a business-value problem rather than merely a technical prediction problem. This perspective is consistent with research showing that privacy has measurable economic consequences for digital service design (Acquisti et al., 2016). This article therefore treats privacy controls as part of the operating architecture, not as a peripheral compliance add-on (Lu and Xu, 2019). The need for a balanced privacy-utility view is reinforced by federated learning studies that treat heterogeneity and deployment constraints as core design issues (Yuan et al., 2011).

Traditional platform analytics usually begins with a centralized data lake. Raw trip logs, delivery traces, routing histories, and app interactions are aggregated on platform servers, where data scientists train demand forecasting, dispatch, pricing, fraud detection, and customer retention models. Centralization simplifies experimentation and often produces strong short-run model performance, but it also concentrates on privacy and security exposure. When raw mobility data are pooled, the platform increases its obligations under privacy law, raises the cost of breach prevention, and increases the reputational damage that follows any misuse of data. For platform operations, the relevant question is therefore not whether mobility data have value; the relevant question is how much value remains after privacy risk, communication cost, compliance cost, and stakeholder trust are included in the operating calculus. The technical premise also follows the broader movement toward distributed and privacy-aware learning architectures (Yang et al., 2019). Evidence from intelligent systems research also suggests that algorithmic capability must be interpreted together with institutional and technological context (Malhotra et al., 2004). Platform governance research similarly indicates that value is created through ecosystem-level coordination rather than isolated technical optimization (Yang et al., 2025).

Federated learning offers a promising architecture for this problem because it trains models across distributed devices or organizational nodes without requiring raw data to be transferred to a central platform. The uploaded PDF manuscript that motivates this study develops a privacy-preserving federated learning framework for mobility data mining and emphasizes differential privacy, secure aggregation, communication compression, and personalization under non-independent mobility distributions. This article shifts the analytical focus from algorithmic performance alone to business value in platform operations. The central argument is that mobility analytics should be evaluated through a federated risk-utility lens: prediction accuracy must be balanced against privacy exposure, communication cost, trust effects, and operational risk

 https://doi.org/10.63646/jbda.2025.030204

reduction. For platform operators, analytics value depends on whether data-driven decisions improve operational performance rather than only model accuracy (Choi et al., 2018). This perspective is consistent with research showing that privacy has measurable economic consequences for digital service design (Tiwana et al., 2010). This article therefore treats privacy controls as part of the operating architecture, not as a peripheral compliance add-on (Zuboff, 2015).

The proposed framework is called FedRU, a federated risk-utility framework for platform operations. It is not intended to replace technical federated learning algorithms. Rather, it provides a business analytics layer that helps managers decide when privacy-preserving mobility analytics creates value, when strict privacy controls reduce utility too much, and when a centralized data strategy becomes financially or ethically fragile. The framework uses scenario analysis, operational metrics, and risk-adjusted value indicators to compare centralized analytics, local-only analytics, basic federated learning, differentially private federated learning, and a governed federated design that combines privacy safeguards with value gates. Related work on information systems and digital finance further shows that data infrastructures reshape market coordination and risk assessment (Kou and Lu, 2025). The technical premise also follows the broader movement toward distributed and privacy-aware learning architectures (Xu et al., 2024). Evidence from intelligent systems research also suggests that algorithmic capability must be interpreted together with institutional and technological context (Luca et al., 2021).

This study contributes to literature and practice in four ways. First, it translates privacy-preserving mobility learning into platform operations language by linking model design choices to dispatch quality, customer trust, compliance loss, communication cost, and risk-adjusted operating value. Second, it provides a structured scenario design that allows platform managers to compare analytics architectures under common metrics rather than relying on accuracy alone. Third, it offers a data-analysis illustration showing that the strongest business value does not necessarily come from the highest predictive accuracy; it comes from the best balance between model utility and privacy risk. Fourth, it proposes governance thresholds that can be embedded into dashboards for platform operations teams, privacy officers, and data science managers. The remainder of the article reviews the relevant literature, develops the framework, presents the numerical analysis, and discusses managerial implications for privacy-sensitive mobility platforms. The need for a balanced privacy-utility view is reinforced by federated learning studies that treat heterogeneity and deployment constraints as core design issues (Kairouz et al., 2021). For platform operators, analytics value depends on whether data-driven decisions improve operational performance rather than only model accuracy (Smith et al., 2011).

## 2. Literature Review

### 2.1 Mobility Analytics and Platform Operations

Mobility analytics has evolved from descriptive mapping into a core mechanism of platform coordination. Early research on human mobility documented the strong regularities in individual movement patterns, showing that location traces can support prediction but also create obvious privacy concerns because regularity makes individuals identifiable (Gonzalez et al., 2008). Subsequent work in trajectory data mining clarified how spatiotemporal data can be segmented, clustered, matched to road networks, and transformed into features for prediction, recommendation,

and anomaly detection (Zheng, 2015). For platform operations, these methods support real-time demand sensing, dispatch matching, route recommendation, delivery scheduling, and service reliability monitoring. Platform governance research similarly indicates that value is created through ecosystem-level coordination rather than isolated technical optimization (Gawer, 2014). Related work on information systems and digital finance further shows that data infrastructures reshape market coordination and risk assessment (Gunasekaran et al., 2017).

The value of mobility analytics differs across platform service lines. Ride-hailing platforms use mobility data to reduce pickup delay, balance driver supply, and maintain reliability under demand surges. On-demand delivery platforms use courier traces, merchant waiting time, and drop-off density to allocate drivers and estimate delivery windows. Urban courier platforms use route density, depot congestion, and enterprise service commitments to manage operational capacity. Shared-mobility platforms use vehicle availability, parking station flows, and trip completion patterns to rebalance assets. Across these settings, mobility analytics has business value because it reduces variance: it narrows the gap between expected and realized demand, between promised and actual delivery time, and between planned and available capacity. This article therefore treats privacy controls as part of the operating architecture, not as a peripheral compliance add-on (Li et al., 2020). The need for a balanced privacy-utility view is reinforced by federated learning studies that treat heterogeneity and deployment constraints as core design issues (Lu, 2018).

However, platform operations are not only optimization systems. They are institutional systems that depend on trust. Customers, workers, merchants, and partner organizations must believe that mobility data are used within acceptable boundaries. If a platform maximizes dispatch accuracy by collecting excessively granular movement histories, the immediate operating gain may be offset by opt-outs, regulatory penalties, public criticism, or increased cybersecurity exposure. In economic terms, raw mobility data generates both decision value and liability value. A sustainable platform analytics design must capture the former while controlling the latter. Evidence from intelligent systems research also suggests that algorithmic capability must be interpreted together with institutional and technological context (Lu, 2025). Platform governance research similarly indicates that value is created through ecosystem-level coordination rather than isolated technical optimization (Dinev and Hart, 2006).

## 2.2 Federated Learning and Privacy-Preserving Analytics

Federated learning was developed to support distributed model training when raw data remains on local clients. Instead of pooling training records, a central coordinator sends a model to participating nodes, local nodes train on their own data, and only model updates are aggregated. The original federated averaging method demonstrated that communication-efficient model training was feasible across decentralized data sources (McMahan et al., 2017). Later surveys emphasized that federated learning is attractive in mobile and edge environments because data are naturally distributed, devices are intermittently available, and privacy constraints are strong (Kairouz et al., 2021; Lim et al., 2020). These features are especially relevant to urban mobility platforms, where drivers, couriers, customer devices, depots, and merchant terminals generate data under heterogeneous conditions. This perspective is consistent with research showing that privacy has measurable economic consequences for digital service design (Bonawitz et al., 2017). This article therefore treats privacy controls as part of the operating architecture, not as a peripheral

compliance add-on (Queiroz et al., 2020).

Federated learning alone does not eliminate privacy risk. Model updates can leak information about local data, especially when adversaries observe gradients, combine updates over time, or exploit rare features (Melis et al., 2019; Nasr et al., 2019). Differential privacy reduces this risk by adding calibrated noise and limiting the influence of any single record (Dwork, 2006; Abadi et al., 2016). Secure aggregation adds another layer by allowing the server to aggregate local updates without seeing any individual update in plaintext (Bonawitz et al., 2017). Communication compression, such as sparsification or quantization, lowers bandwidth cost and makes federated learning more practical for mobile or edge deployment. Personalization addresses non-independent and heterogeneous data by allowing local models or local adjustments to represent different mobility contexts, such as dense downtown demand, suburban commuting, or airport-related flows. The technical premise also follows the broader movement toward distributed and privacy-aware learning architectures (Akter et al., 2016). Evidence from intelligent systems research also suggests that algorithmic capability must be interpreted together with institutional and technological context (Xu et al., 2011).

The uploaded PDF manuscript is aligned with this technical tradition. Its mobility mining framework integrates differential privacy, secure aggregation, gradient compression, and personalized aggregation to keep raw location traces on devices while maintaining predictive utility. The present article uses that research direction as a foundation but reframes the problem for business and data analytics. Instead of asking only whether a federated mobility model improves accuracy or reduces communication overhead, it asks how those technical effects translate into platform value, risk reduction, and governance decisions. For platform operators, analytics value depends on whether data-driven decisions improve operational performance rather than only model accuracy (Dwork and Roth, 2014). This perspective is consistent with research showing that privacy has measurable economic consequences for digital service design (Lu, 2017a).

## 2.3 Business Value, Data Risk, and Risk-Utility Trade-Offs

The economics of privacy suggests that data-driven firms must evaluate privacy not only as a legal requirement but also as a factor in market performance (Acquisti et al., 2016; Goldfarb & Tucker, 2019). Stronger privacy safeguards may reduce data access, experimentation speed, or model detail, but they may also reduce breach exposure, increase willingness to share data, and protect long-run brand value. In platform markets, this trade-off is complicated by network effects. If customers and workers trust the platform, they may participate more fully, which increases data coverage and improves model quality. If they distrust the platform, they may opt out, provide less accurate information, or switch to competitors, which reduces both operational efficiency and data value. Related work on information systems and digital finance further shows that data infrastructures reshape market coordination and risk assessment (Xu et al., 2021). The technical premise also follows the broader movement toward distributed and privacy-aware learning architectures (Chen et al., 2012).

Business analytics research has often measured value through forecast accuracy, cost reduction, revenue lift, or customer retention. For privacy-preserving mobility analytics, those measures are necessary but incomplete. A model with the highest ETA accuracy may not create the highest

business value if it depends on centralized raw trace storage, excessive retention, or weak partner controls. Conversely, an extremely strict privacy design may protect data but leave operations fragmented and unreliable. Risk-adjusted utility is therefore a better lens. It treats analytics value as a composite outcome that includes prediction utility, privacy risk, communication cost, compliance cost, and trust capital. The need for a balanced privacy-utility view is reinforced by federated learning studies that treat heterogeneity and deployment constraints as core design issues (Wamba et al., 2017). For platform operators, analytics value depends on whether data-driven decisions improve operational performance rather than only model accuracy (Lu, 2017b).

This study adopts a practical interpretation of risk-utility rather than a purely formal mathematical one. Managers do not always have reliable estimates of every privacy loss parameter, breach probability, or customer response. They do, however, have operational indicators: model error, average pickup delay, route deviation rate, data opt-out rate, network latency, complaint rate, and audit findings. The proposed FedRU framework organizes these indicators into a decision structure that helps platform managers choose an analytics architecture suited to their risk profile and operating constraints. Platform governance research similarly indicates that value is created through ecosystem-level coordination rather than isolated technical optimization (Mothukuri et al., 2021). Related work on information systems and digital finance further shows that data infrastructures reshape market coordination and risk assessment (Constantiou and Kallinikos, 2015).

## 3. Methodology and Framework Design

This study develops a conceptual and numerical business analytics framework rather than a new low-level federated learning algorithm. The research design follows a scenario-comparison approach. Five analytics architectures are evaluated under a common operating setting for an urban mobility platform. Each architecture is assessed using a set of business and risk indicators: prediction utility, privacy exposure, communication cost, expected regulatory loss, customer trust, and risk-adjusted operating value. The numerical values are simulated for analytical illustration and calibrated to typical patterns discussed in mobility analytics and federated learning research, including heterogeneous clients, privacy-utility trade-offs, and communication constraints. This article therefore treats privacy controls as part of the operating architecture, not as a peripheral compliance add-on (Grover et al., 2018). The need for a balanced privacy-utility view is reinforced by federated learning studies that treat heterogeneity and deployment constraints as core design issues (Yuan et al., 2010).

The platform environment is defined broadly. It includes ride-hailing, on-demand delivery, urban courier services, and shared-mobility operations. Each service line uses location data, but each line has different value mechanisms and different privacy risks. The framework assumes that the platform must continuously update operational models for ETA prediction, demand forecasting, route planning, and service-level risk detection. It also assumes that raw mobility traces are sensitive, and that centralized storage increases exposure to data misuse, breach costs, and regulatory scrutiny. These assumptions reflect the practical environment faced by many data-intensive platform businesses. Evidence from intelligent systems research also suggests that algorithmic capability must be interpreted together with institutional and technological context (Wu et al., 2025). Platform governance research similarly indicates that value is created through

ecosystem-level coordination rather than isolated technical optimization (Lu and Zheng, 2020).

**Table 1. Risk-Utility Constructs for Platform Mobility Analytics**

| Construct | Operational meaning | Platform decision supported | Expected business value |
|---|---|---|---|
| Prediction utility | Accuracy and stability of ETA, demand, and dispatch models | Fleet balancing, surge moderation, courier allocation | Higher service reliability and lower idle time |
| Privacy exposure | Probability and cost of inferring individual location traces from analytics outputs | Privacy budget, local training scope, data retention policy | Lower regulatory and reputational loss |
| Communication efficiency | Bandwidth and round-time required to train or update distributed models | Compression level, update frequency, edge participation rules | Lower infrastructure cost and faster model refresh |
| Operational risk | Loss from poor matching, wrong route prediction, or stale demand signals | Alert thresholds, manual review, escalation paths | Fewer SLA breaches and better customer retention |
| Trust capital | Stakeholder willingness to share data under credible safeguards | Consent design, partner transparency, audit reporting | Greater data coverage without raw-data centralization |

Table 1 summarizes the constructions used in the framework. The table is intentionally managerial rather than purely technical. It connects data science design choices with operational decisions, such as whether to refresh a model more frequently, adjust privacy budgets, compress updates, or invest in auditability. This structure is important because platform managers rarely evaluate analytics architectures using one metric. A realistic decision requires trade-offs among service quality, privacy, cost, and trust.

The canvas emphasizes that governance does not sit outside analytics. Privacy budgets, secure aggregation, audit logs, and stakeholder communication shape the data coverage available to the platform. Better governance can increase willingness to participate, which may improve model quality even when direct access to raw traces is reduced. This is the central business logic behind federated mobility analytics: the platform may sacrifice a small amount of short-term modeling convenience while gaining lower exposure, higher trust, and more sustainable data access.

## 3.1 Scenario Construction and Numerical Design

The empirical component of this article uses numerical scenario analysis. The purpose is not to report a proprietary field experiment but to demonstrate how platform managers can compare analytics architectures under a consistent risk-utility lens. The analysis begins with a centralized raw-data baseline, adds a local-only alternative, and then evaluates three federated designs with increasing governance strength. The metric values are presented as standardized indices from 0 to 100. Higher values indicate better prediction utility, stronger trust, or higher risk-adjusted operating value, but higher values of privacy exposure and communication cost indicate worse outcomes. This perspective is consistent with research showing that privacy has measurable economic consequences for digital service design (Abadi et al., 2016). This article therefore treats privacy controls as part of the operating architecture, not as a peripheral compliance add-on (Günther et al., 2017).

**Table 2. Scenario Design for Analytics Architecture Comparison**

| Scenario | Learning design | Privacy control | Analytics utility assumption | Main business risk |
|---|---|---|---|---|
| S0 Centralized raw- | Raw traces pooled in a | Access control only | High short-run utility | High breach, consent, |

 https://doi.org/10.63646/jbda.2025.030204

| | | | | |
|---|---|---|---|---|
| data analytics | platform data lake | | | and compliance exposure |
| S1 Local-only analytics | Each node estimates local demand independently | Data remains fully local | Low cross-region generalization | Fragmented decisions and inconsistent service quality |
| S2 Basic federated learning | Client updates aggregated centrally | Raw data remains local | High utility under moderate heterogeneity | Gradient leakage and uneven client quality |
| S3 Differentially private FL | Federated updates with calibrated noise | Privacy budget and clipping rules | Moderate utility with stronger privacy | Utility loss when noise is over-calibrated |
| S4 Governed FedRU framework | Federated learning with privacy, secure aggregation, compression, and value gates | DP, secure aggregation, audit logs, and governance dashboard | High risk-adjusted utility | Residual cost of governance and model monitoring |

Table 2 shows that the scenarios differ not only in technical privacy controls but also in managerial accountability. Basic federated learning prevents raw trace pooling, but it does not necessarily provide strong protection against gradient leakage or weak partner governance. Differentially private federated learning reduces exposure, but excessive noise may reduce operational utility. The governed FedRU scenario combines technical safeguards with value gates that prevent the platform from treating accuracy as the only success criterion.

## 4. Results and Data Analysis

### 4.1 Comparative Analytics Architecture Outcomes

The scenario analysis indicates that centralized raw-data analytics has strong prediction utility but weak risk-adjusted performance. Centralized analytics reaches a prediction utility index of 91.5, which is the highest value among all scenarios. Yet its privacy exposure index is 92.0, and its expected regulatory loss index is 44.0. This means that centralized analytics creates a large amount of operating knowledge at the cost of concentrating sensitive traces. For a platform facing strict privacy regulation, competitive scrutiny, or reputational vulnerability, this concentration of raw mobility data becomes a major business liability. The technical premise also follows the broader movement toward distributed and privacy-aware learning architectures (Goldfarb and Tucker, 2019). Evidence from intelligent systems research also suggests that algorithmic capability must be interpreted together with institutional and technological context (Lu and Ning, 2020).

The local-only scenario minimizes privacy exposure, but it produces weak cross-region learning. Its prediction utility index is 78.2, and its risk-adjusted operating value is only 66.5. This outcome is intuitive: when each node learns independently, the platform loses the benefit of cross-district, cross-merchant, and cross-fleet patterns. A courier depot may understand its own local delivery rhythms, but it cannot learn from similar demand shocks in other districts. A ride-hailing submarket may estimate pickup delay in its own zone, but it cannot borrow statistical strength from comparable zones. Local-only learning therefore protects privacy but limits the network-level intelligence that platforms need. For platform operators, analytics value depends on whether data-driven decisions improve operational performance rather than only model accuracy (Zheng, 2015). This perspective is consistent with research showing that privacy has measurable economic consequences for digital service design (Huang and Rust, 2021).

Basic federated learning improves the balance. It reaches a prediction utility index of 89.7 and a risk-adjusted operating value of 83.8. This shows that distributed learning can preserve much of

the value of centralized analytics while avoiding raw trace pooling. However, the privacy exposure index remains 36.0, which is lower than centralization but not negligible. The exposure comes from model updates, gradient patterns, rare-feature leakage, and uneven client participation. For a mobility platform with sensitive trajectories, basic federated learning should be considered a useful starting point but not a complete governance solution. Related work on information systems and digital finance further shows that data infrastructures reshape market coordination and risk assessment (Chen et al., 2024). The technical premise also follows the broader movement toward distributed and privacy-aware learning architectures (Zheng and Lu, 2022).

**Table 3. Scenario Results for Risk-Adjusted Platform Analytics**

| Metric | S0 Centralized | S1 Local only | S2 Basic FL | S3 DP-FL | S4 Governed FedRU |
|---|---|---|---|---|---|
| Prediction utility index | 91.5 | 78.2 | 89.7 | 87.8 | 89.1 |
| Privacy exposure index | 92.0 | 18.0 | 36.0 | 24.0 | 15.0 |
| Communication cost index | 68.0 | 22.0 | 54.0 | 56.0 | 39.0 |
| Expected regulatory loss index | 44.0 | 9.0 | 19.0 | 12.0 | 7.0 |
| Customer trust index | 52.0 | 74.0 | 68.0 | 79.0 | 86.0 |
| Risk-adjusted operating value | 79.2 | 66.5 | 83.8 | 81.4 | 88.7 |

Table 3 shows the central finding of the analysis. The governed FedRU architecture produces the highest risk-adjusted operating value, even though it does not produce the highest prediction utility. Its prediction utility index is 89.1, below the centralized score of 91.5, but its privacy exposure index is only 15.0, and its customer trust index is 86.0. The platform therefore gains a more sustainable form of value. It keeps enough predictive power to support dispatch, routing, and demand sensing while reducing the downside risks associated with raw trace centralization.

Figure 1 visualizes this result by comparing prediction utility, privacy exposure, and risk-adjusted value. The figure makes the trade-off visible. Centralized analytics is strong on utility but weak on exposure. Local-only analytics is strong on exposure but weak on utility. The governed FedRU design is not extreme on any single dimension; instead, it is the best joint design. This matters for business analytics because platform value depends on multiple stakeholders. Customers care about convenience and privacy. Workers care about fair allocation and surveillance boundaries. Partners care about data leakage and commercial confidentiality. Regulators care about necessity, proportionality, and accountability.

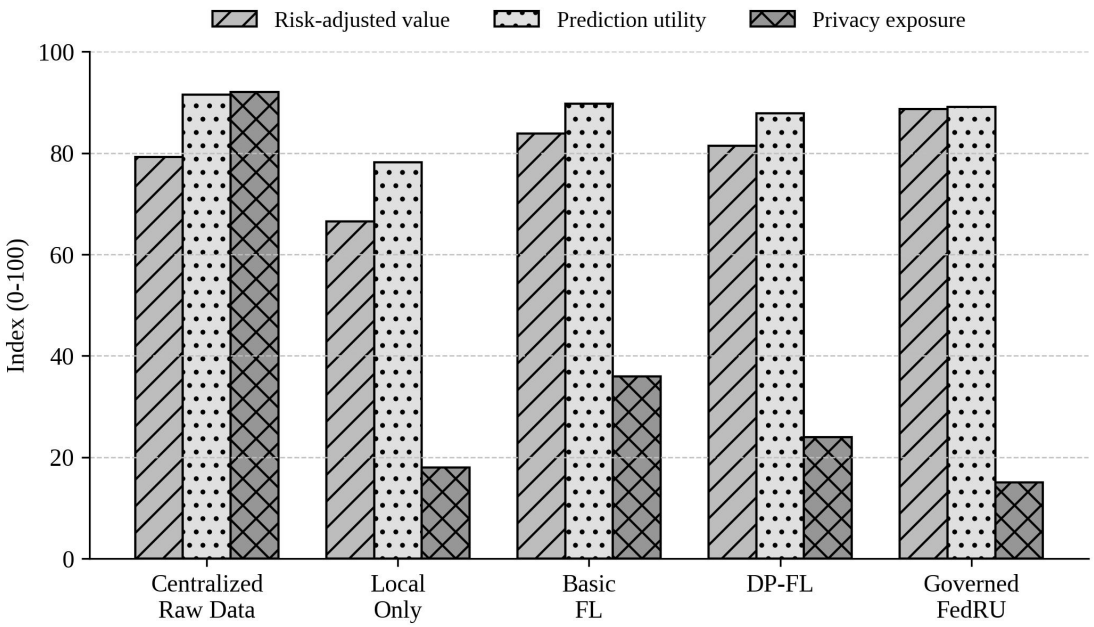


**Figure 1. Scenario comparison of prediction utility, privacy exposure, and risk-adjusted operating value.**

The scenario comparison also reveals that communication cost cannot be ignored. Basic federated learning has a communication cost index of 54.0, reflecting the cost of repeated model-update exchange. Differentially private federated learning raises this cost slightly to 56.0 because privacy control may require additional coordination, clipping, accounting, and monitoring. The governed FedRU design reduces the cost index to 39.0 by incorporating compression and asynchronous participation. In business terms, communication efficiency is not just an engineering metric; it affects model refresh frequency, infrastructure budget, and the speed with which operational teams can respond to changing urban conditions. The need for a balanced privacy-utility view is reinforced by federated learning studies that treat heterogeneity and deployment constraints as core design issues (Ivanov and Dolgui, 2021). For platform operators, analytics value depends on whether data-driven decisions improve operational performance rather than only model accuracy (Rieke et al., 2020).

## 4.2 Privacy-Utility Balance

A second analysis examines privacy-budget settings and their implications for business value. In federated learning with differential privacy, a stricter privacy budget usually reduces exposure but can also reduce utility when noise obscures useful signals. A looser privacy budget can improve prediction performance but may increase privacy risk. The platform must therefore identify a governance threshold where the marginal gain in utility no longer justifies the marginal increase in privacy exposure. This is a business governance problem because the threshold depends on regulatory context, stakeholder expectations, and the financial value of improved prediction. Platform governance research similarly indicates that value is created through ecosystem-level coordination rather than isolated technical optimization (Lim et al., 2020). Related work on information systems and digital finance further shows that data infrastructures reshape market coordination and risk assessment (Lu et al., 2020).

Figure 2 shows that model utility rises as the privacy budget becomes looser, but the increase flattens after a moderate level. Privacy-risk exposure, by contrast, rises steadily. Net business value peaks near the governance threshold used in the analysis. This result supports a pragmatic privacy strategy. The platform should not adopt the strictest possible setting automatically, because overly strict privacy controls may damage service reliability. It also should not adopt the loosest possible setting simply to maximize accuracy, because the incremental operating gain may be outweighed by privacy risk and trust loss. The right setting is the one that produces the strongest net value under governance constraints.

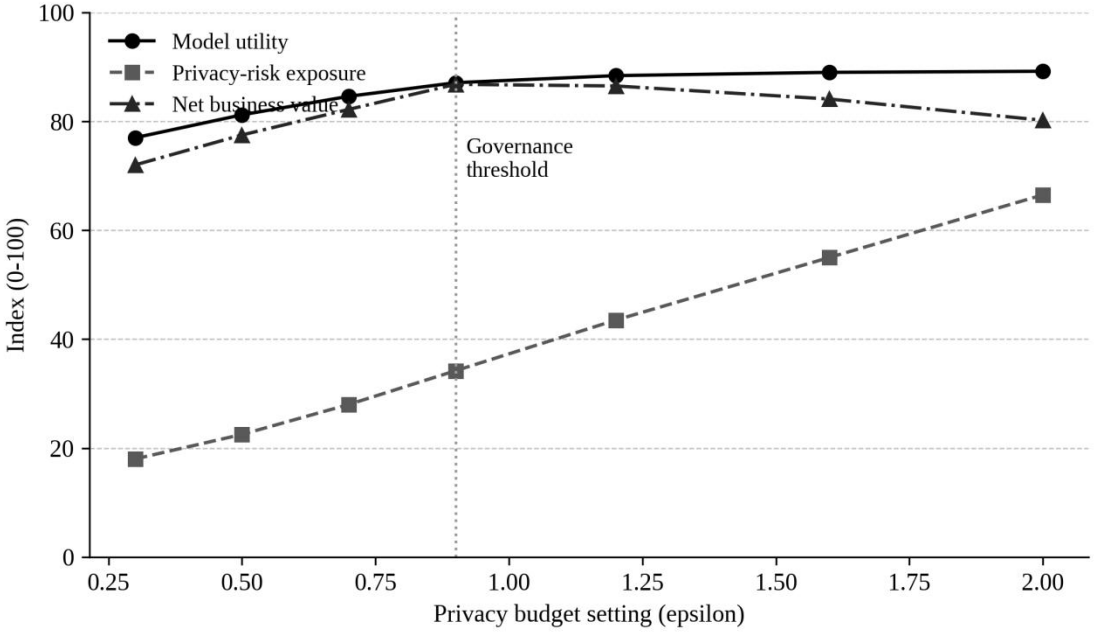


**Figure 2. Privacy-utility sensitivity analysis for federated mobility analytics.**

The implication for platform operations is direct. Privacy settings should be monitored alongside dispatch performance, delivery delay, customer complaints, and data participation rates. When model utility falls below a governance threshold, the platform should first inspect whether excessive noise, overly narrow client participation, or poor segmentation is responsible. When privacy exposure rises above a threshold, the platform should reduce the privacy budget, increase clipping, remove sensitive features, or apply stricter aggregation. A privacy-preserving analytics system is therefore not a one-time deployment. It is an adaptive operating capability. This article therefore treats privacy controls as part of the operating architecture, not as a peripheral compliance add-on (Rysman, 2009). The need for a balanced privacy-utility view is reinforced by federated learning studies that treat heterogeneity and deployment constraints as core design issues (Melis et al., 2019).

## 4.3 Service-Line Analysis

The business value of privacy-preserving mobility analytics also varies across service lines. Ride-hailing platforms benefit most from improved ETA prediction, real-time supply balancing, and pickup matching. On-demand delivery platforms benefit from merchant waiting-time prediction, drop-off reliability, and courier allocation. Urban courier platforms benefit from depot-

level route density and enterprise service reliability. Shared-mobility platforms benefit from vehicle rebalancing and station-level demand forecasts. Each service line has a different privacy-sensitive element, which means that the same federated architecture may require different data governance rules across operations. Evidence from intelligent systems research also suggests that algorithmic capability must be interpreted together with institutional and technological context (Zhang and Lu, 2021). Platform governance research similarly indicates that value is created through ecosystem-level coordination rather than isolated technical optimization (Ye and Lu, 2022).

**Table 4. Service-Line Value Mechanisms for Privacy-Preserving Mobility Analytics**

| Service line | Dominant mobility data | Primary operating value | Privacy-sensitive element | FedRU value mechanism |
|---|---|---|---|---|
| Ride-hailing | Driver location, passenger pickup, ETA history | Lower pickup delay and better driver utilization | Home-work pattern and night mobility | Neighborhood-level matching without raw trace pooling |
| On-demand delivery | Courier movement, merchant wait time, drop-off density | Shorter delivery windows and fewer failed drops | Customer residence, workplace, and purchase rhythm | Federated demand learning across merchants and districts |
| Urban courier platform | Parcel route, depot status, traffic encounter | Higher route density and lower re-routing cost | Enterprise client locations and contractual volumes | Secure aggregation among depots and carrier partners |
| Shared mobility | Vehicle availability, parking station flow, trip completion | Improved rebalancing and fewer stockouts | Station habits and commuter cycles | Risk-aware rebalancing without user-level trace exposure |

Table 4 highlights the importance of aligning analytics governance with operating context. For ride-hailing, home-work movement regularity is a sensitive feature, so model inputs should be aggregated, clipped, or locally transformed before update sharing. For delivery, customer residence and purchase rhythm create privacy sensitivity, especially when food, medicine, or late-night orders are involved. For urban courier platforms, enterprise client locations and delivery volumes may reveal commercial information. For shared mobility, commuter cycles and station habits may expose individual routines. A platform-wide federated architecture should therefore include service-specific feature policies rather than a single generic privacy policy.

## 5. Discussion

### 5.1 Why Risk-Adjusted Value Exceeds Accuracy as a Business Metric

The most important managerial lesson is that accuracy is not a sufficient measure of platform analytics value. Centralized raw-data analytics produces the strongest prediction utility in the scenario analysis, but it does not produce the strongest business value. This result is not paradoxical. Accuracy is a local property of a model, while business value is a system property of an operating organization. The system includes customers, workers, merchants, regulators, cloud infrastructure, security teams, and public trust. A model that performs well in isolation can become less valuable once the cost of privacy exposure, breach prevention, litigation, regulatory response, and stakeholder resistance is included. This perspective is consistent with research showing that privacy has measurable economic consequences for digital service design (Nguyen et al., 2021). This article therefore treats privacy controls as part of the operating architecture, not as a peripheral compliance add-on (Martin, 2015).

The FedRU framework reframes privacy-preserving analytics as a value engineering problem. Privacy controls are not simply constraints that reduce model utility. In some contexts, they protect

the conditions under which data-driven operations remain legitimate and scalable. If strong privacy safeguards reduce opt-outs and increase partner willingness to participate, the platform may eventually have broader and more representative data coverage than a platform that uses aggressive centralized data collection. This possibility is especially relevant in urban mobility, where local governments, unions, enterprise clients, and privacy advocates may influence data access arrangements. The technical premise also follows the broader movement toward distributed and privacy-aware learning architectures (Gonzalez et al., 2008). Evidence from intelligent systems research also suggests that algorithmic capability must be interpreted together with institutional and technological context (Lu et al., 2023).

## 5.2 Business Value Decomposition

The business value of the governed federated design comes from several sources. The first is direct operational value: better demand forecasts, more accurate ETA predictions, fewer failed deliveries, and improved asset utilization. The second is risk reduction: lower probability that sensitive traces are misused, breached, or inferred from analytics outputs. The third is communication efficiency: compression and asynchronous updates lower infrastructure cost and make model refreshes more feasible. The fourth is trust capital: a platform that can explain how it learns from mobility data without centralizing raw traces may reduce customer resistance and partner data withholding. The fifth is compliance readiness: audit logs, privacy budgets, and access controls support regulatory communication and internal accountability. For platform operators, analytics value depends on whether data-driven decisions improve operational performance rather than only model accuracy (Dubey et al., 2019). This perspective is consistent with research showing that privacy has measurable economic consequences for digital service design (Kaissis et al., 2020).

Figure 3 presents this logic as a waterfall analysis. The baseline analytics value begins at 100. Privacy controls impose an initial cost because the platform loses some convenience and must manage additional governance overhead. However, lower data risk, communication compression, trust and retention effects, and audit benefits jointly produce a higher net value. The specific numbers are illustrative, but the mechanism is general. Platforms should not assume that privacy safeguards only reduce value. Well-designed safeguards may increase net value by reducing risk and increasing participation.

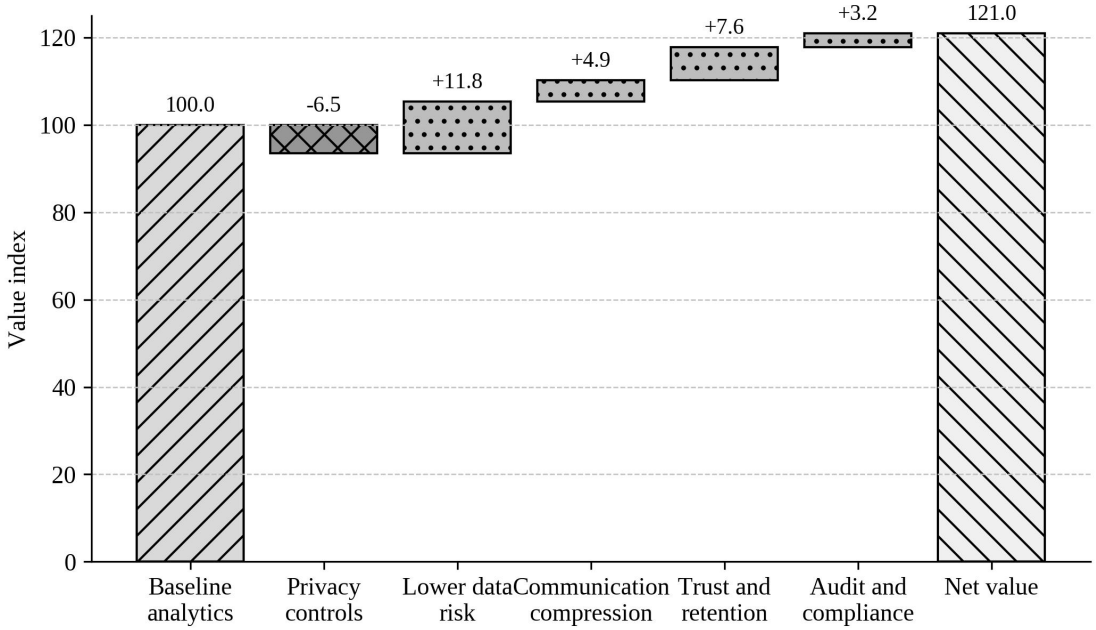


**Figure 3. Business value waterfall for governed federated mobility analytics.**

The waterfall also clarifies why governance should be evaluated with data. If privacy controls are too strict, the initial utility loss may exceed the risk reduction. If controls are too loose, the privacy exposure may erase the value generated by better predictions. If communication compression is too aggressive, model quality may deteriorate. If audit reporting is superficial, it may not increase trust. The goal is therefore to create a feedback loop in which platform managers observe both operating performance and governance performance, then adjust technical settings accordingly. Related work on information systems and digital finance further shows that data infrastructures reshape market coordination and risk assessment (Lu, 2019a). The technical premise also follows the broader movement toward distributed and privacy-aware learning architectures (Lu et al., 2024a).

## 5.3 Governance Thresholds for Platform Managers

A practical implementation of the FedRU framework requires thresholds. Thresholds translate abstract risk-utility reasoning into operational rules. Table 5 proposes a dashboard structure that platform managers can adapt to their own data environment. The threshold categories include privacy exposure, prediction utility, communication cost, stakeholder trust, and risk-adjusted value. The purpose is not to replace statistical validation. The purpose is to ensure that model deployment decisions are not made solely by the data science team or solely by the legal team. They should be made through a joint operating governance process. The need for a balanced privacy-utility view is reinforced by federated learning studies that treat heterogeneity and deployment constraints as core design issues (Hagiu and Wright, 2015). For platform operators, analytics value depends on whether data-driven decisions improve operational performance rather than only model accuracy (Truong et al., 2021).

**Table 5. Governance Dashboard Thresholds for Federated Platform Operations**

| Governance threshold | Observed signal | Recommended platform | Business interpretation |
|---|---|---|---|

 https://doi.org/10.63646/jbda.2025.030204

| | | action | |
|---|---|---|---|
| Privacy exposure above 25 | Membership inference or abnormal gradient similarity rises | Lower privacy budget, increase clipping, restrict high-risk features | The platform is buying utility with excessive privacy risk |
| Prediction utility below 84 | ETA and demand forecast error increases across two rounds | Relax excessive noise, increase client participation, recalibrate segments | Privacy controls are undermining operational performance |
| Communication cost above 50 | Bandwidth and round latency exceed budget | Apply top-k compression and asynchronous participation | Infrastructure cost is reducing the value of frequent model refresh |
| Trust index below 75 | Opt-out rate or partner data withholding increases | Publish audit metrics and simplify consent explanations | Stakeholders do not understand or believe the privacy design |
| Risk-adjusted value below 80 | Combined value score falls despite high model accuracy | Review governance balance rather than model accuracy alone | Accuracy is not sufficient when compliance and trust costs dominate |

Table 5 can be read as a decision guide. When privacy exposure is too high, the response should focus on privacy mechanisms, feature limits, and aggregation rules. When prediction utility is too low, the response should examine whether privacy noise is excessive or whether the client population is not representative. When communication cost is too high, the response should focus on compression and update scheduling. When trust is too low, the response should focus on consent design, audit reporting, and stakeholder communication. When risk-adjusted value is low despite high accuracy, the platform should recognize that accuracy is not solving the real business problem.

# 6. Managerial and Theoretical Implications

## 6.1 Implications for Platform Operations

For platform managers, the first implication is that privacy-preserving mobility analytics should be treated as an operating capability rather than a compliance add-on. If privacy controls are added only after a model is built, they are likely to appear as obstacles. If they are designed into analytics architecture from the beginning, they become part of the value proposition. A platform can then state that it learns from aggregate mobility patterns while avoiding unnecessary centralization of raw personal trajectories. This statement has operational relevance because it can support partner onboarding, public-sector collaboration, and customer trust. Platform governance research similarly indicates that value is created through ecosystem-level coordination rather than isolated technical optimization (Aledhari et al., 2020). Related work on information systems and digital finance further shows that data infrastructures reshape market coordination and risk assessment (Lu et al., 2024b).

The second implication is that platform analytics teams should use risk-adjusted performance dashboards. A model deployment review should include prediction performance, communication burden, privacy exposure, inference-risk tests, client participation, opt-out trends, and customer complaint signals. The review should be repeated over time because urban conditions change. Demand shocks, holidays, weather events, road closures, public events, and competitor promotions may all alter the value-risk balance. A privacy setting that is acceptable in a stable month may become problematic during a high-demand festival if it degrades dispatch reliability, while a setting that is acceptable in a pilot may become risky at citywide scale. This article therefore treats privacy controls as part of the operating architecture, not as a peripheral compliance add-on (Ben-Daya et al., 2019). The need for a balanced privacy-utility view is reinforced by federated learning studies

that treat heterogeneity and deployment constraints as core design issues (Huang and Swaminathan, 2009).

The third implication is that service-line heterogeneity requires governance differentiation. A single privacy budget or update frequency may not fit ride-hailing, food delivery, enterprise courier, and shared mobility operations simultaneously. B2B courier data may reveal commercial relationships and contract volumes. Food delivery data may reveal sensitive consumption and household patterns. Ride-hailing data may expose work schedules and social routines. Shared-mobility data may reveal commuting habits. A mature platform should create service-line privacy profiles and connect them to model settings. Evidence from intelligent systems research also suggests that algorithmic capability must be interpreted together with institutional and technological context (Lu and Yang, 2024). Platform governance research similarly indicates that value is created through ecosystem-level coordination rather than isolated technical optimization (Lu et al., 2024c).

## 6.2 Implications for Business and Data Analytics Research

For business analytics research, this article shows the value of connecting privacy-preserving machine learning with managerial performance measurement. Federated learning research often reports accuracy, convergence, communication rounds, and privacy parameters. These metrics are necessary, but they do not fully explain why a platform should invest in a privacy-preserving architecture. Business and data analytics research can extend this work by estimating the relationship between privacy governance and customer participation, between trust and data coverage, and between privacy incidents and operating cost. These relationships would allow future studies to calculate risk-adjusted data value more precisely. This perspective is consistent with research showing that privacy has measurable economic consequences for digital service design (Culnan and Armstrong, 1999). This article therefore treats privacy controls as part of the operating architecture, not as a peripheral compliance add-on (Belanger and Crossler, 2011).

The framework also contributes to the literature on digital platforms. Platforms are often described as data-intensive intermediaries that create value by coordinating multiple sides of a market. The mobility platform context shows that data intensity has a boundary: too much centralized raw data can produce liability, not just value. The optimal analytics architecture may therefore be less centralized than traditional platform economics might imply. Federated learning, secure aggregation, and privacy-aware governance can be interpreted as institutional mechanisms that allow platforms to continue coordinating activity without demanding unlimited data centralization. The technical premise also follows the broader movement toward distributed and privacy-aware learning architectures (Toorajipour et al., 2021). Evidence from intelligent systems research also suggests that algorithmic capability must be interpreted together with institutional and technological context (Kshetri, 2018).

## 6.3 Robustness Considerations

The numerical analysis is illustrative and should not be interpreted as universal. Different platforms will face different legal environments, model tasks, customer expectations, and infrastructure costs. However, the qualitative result is robust across plausible conditions: a privacy-preserving federated architecture is most valuable when raw-data centralization has high exposure,

when local-only learning loses too much cross-market signal, and when communication cost can be managed through compression and asynchronous updates. If a platform operates in a low-risk environment with minimal privacy sensitivity, centralization may still be economically attractive. If a platform operates in an environment with extreme privacy constraints and low need for cross-location learning, local-only analytics may be sufficient. The FedRU framework helps identify where each condition applies. For platform operators, analytics value depends on whether data-driven decisions improve operational performance rather than only model accuracy (Shokri and Shmatikov, 2015). This perspective is consistent with research showing that privacy has measurable economic consequences for digital service design (Lu, 2021).

Another robustness issue concerns client heterogeneity. Mobility data are highly non-independent. Downtown drivers, suburban commuters, airport fleets, and bicycle couriers generate different patterns. A federated model that does not address heterogeneity may underperform even if it protects privacy. Managers should therefore monitor segment-level utility rather than rely on aggregate accuracy. A system that improves average ETA prediction but worsens prediction for low-income neighborhoods, peripheral districts, or small merchants may create fairness and service quality problems. Personalized federated learning and segment-aware aggregation are important tools for addressing this risk. Related work on information systems and digital finance further shows that data infrastructures reshape market coordination and risk assessment (Lu, 2019b). The technical premise also follows the broader movement toward distributed and privacy-aware learning architectures (Ivanov, 2020).

## 7. Limitations and Future Research

This study has several limitations. First, the numerical values are simulated and standardized to illustrate managerial trade-offs. Future research should apply the framework to real platform data or public mobility benchmarks with operational labels such as pickup delay, delivery failure, or route deviation. Second, the framework does not estimate legal penalties or breach costs from observed incidents. Future work could integrate cyber-risk models and privacy loss accounting with financial loss distributions. Third, the framework treats stakeholder trust as an index, but trust is multidimensional. Customers, drivers, merchants, enterprise clients, and regulators may respond differently to the same privacy-preserving architecture. The need for a balanced privacy-utility view is reinforced by federated learning studies that treat heterogeneity and deployment constraints as core design issues (Martin and Murphy, 2017). For platform operators, analytics value depends on whether data-driven decisions improve operational performance rather than only model accuracy (Zhang and Lu, 2025).

Future research can extend the framework in several directions. One direction is dynamic optimization, where privacy budgets and update frequencies adapt to operating conditions. A second direction is causal evaluation of privacy governance on platform participation, such as whether clearer privacy assurances increase data-sharing consent or reduce driver opt-outs. A third direction is cross-platform comparison, where federated learning enables analytics collaboration among competing mobility platforms or public agencies without direct data pooling. A fourth direction is the integration of fairness metrics, because privacy-preserving analytics can still produce unequal service outcomes if the underlying data are biased or unevenly distributed. Platform governance research similarly indicates that value is created through ecosystem-level

coordination rather than isolated technical optimization (Rochet and Tirole, 2003). Related work on information systems and digital finance further shows that data infrastructures reshape market coordination and risk assessment (McIntyre and Srinivasan, 2017).

## 8. Conclusion

This article developed a federated risk-utility framework for evaluating the business value of privacy-preserving mobility analytics in platform operations. The framework responds to a central tension in platform management: mobility data are valuable because they improve prediction, dispatch, routing, and service reliability, but they are risky because raw trajectories reveal sensitive behavioral patterns. The proposed FedRU framework compares centralized analytics, local-only analytics, basic federated learning, differentially private federated learning, and a governed federated architecture using a common set of business and risk indicators.

The analysis shows that the highest prediction utility is not necessarily the strongest business outcome. Centralized raw-data analytics can produce excellent short-run model performance, but it concentrates privacy exposure and compliance risk. Local-only analytics protects data but fragments decision-making. Basic federated learning improves the balance but leaves residual leakage and governance concerns. The governed federated design produces the strongest risk-adjusted operating value because it combines predictive utility, privacy protection, communication efficiency, auditability, and stakeholder trust. The conclusion is straightforward: platform managers should evaluate mobility analytics through risk-adjusted value rather than accuracy alone.

The article also offers practical guidance. Privacy budgets, secure aggregation, communication compression, client participation, and audit reporting should be monitored as operating variables. Different service lines require different privacy profiles. Governance thresholds should trigger technical and managerial responses before privacy risk or utility loss becomes material. In this sense, privacy-preserving analytics is not a constraint on platform intelligence. It is a strategic approach to sustaining platform intelligence under conditions of trust, regulation, and urban data sensitivity.

## Acknowledgement

The authors thank the anonymous reviewers and editorial team for their constructive comments. The authors also acknowledge the general research communities working on federated learning, mobility analytics, and platform operations, whose contributions shaped the conceptual foundation of this study.

## Declarations

Conflicts of interest: The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this manuscript.

Data availability: No proprietary platform data were used. The numerical values in the scenario analysis are simulated for analytical illustration and can be recreated from the assumptions and tables reported in the manuscript.

Funding: This research received no external funding.

Ethics statement: This study does not involve human participants, animal experiments, identifiable

personal records, or private mobility traces. It uses a conceptual framework and simulated numerical scenarios; therefore, formal ethics approval was not required.

## References

[1] Acquisti, A., Taylor, C., & Wagman, L. (2016). The economics of privacy. Journal of Economic Literature, 54(2), 442-492. https://doi.org/10.1257/jel.54.2.442

[2] Yang, Q., Liu, Y., Chen, T., & Tong, Y. (2019). Federated machine learning: Concept and applications. ACM Transactions on Intelligent Systems and Technology, 10(2), Article 12. https://doi.org/10.1145/3298981

[3] Choi, T. M., Wallace, S. W., & Wang, Y. (2018). Big data analytics in operations management. Production and Operations Management, 27(10), 1868-1883. https://doi.org/10.1111/poms.12838

[4] Kou, G., & Lu, Y. (2025). FinTech: A literature review of emerging financial technologies and applications. Financial Innovation, 11(1), 1-34. https://doi.org/10.1186/s40854-024-00668-6

[5] Kairouz, P., McMahan, H. B., Avent, B., Bellet, A., Bennis, M., Bhagoji, A. N., Bonawitz, K., Charles, Z., Cormode, G., Cummings, R., D'Oliveira, R. G. L., Eichner, H., El Rouayheb, S., Evans, D., Gardner, J., Garrett, Z., Gascon, A., Ghazi, B., Gibbons, P. B., Gruteser, M., Harchaoui, Z., He, C., He, L., Huo, Z., Hutchinson, B., Hsu, J., Jaggi, M., Javidi, T., Joshi, G., Khodak, M., Konecny, J., Korolova, A., Koushanfar, F., Koyejo, S., Lepoint, T., Liu, Y., Mittal, P., Mohri, M., Nock, R., Oh, S., Pagh, R., Qi, H., Ramage, D., Raskar, R., Raykova, M., Song, D., Song, W., Stich, S. U., Sun, Z., Suresh, A. T., Tramer, F., Vepakomma, P., Wang, J., Xiong, L., Xu, Z., Yang, Q., Yu, F. X., Yu, H., & Zhao, S. (2021). Advances and open problems in federated learning. Foundations and Trends in Machine Learning, 14(1-2), 1-210. https://doi.org/10.1561/2200000083

[6] Gawer, A. (2014). Bridging differing perspectives on technological platforms: Toward an integrative framework. Research Policy, 43(7), 1239-1249. https://doi.org/10.1016/j.respol.2014.03.006

[7] Li, T., Sahu, A. K., Talwalkar, A., & Smith, V. (2020). Federated learning: Challenges, methods, and future directions. IEEE Signal Processing Magazine, 37(3), 50-60. https://doi.org/10.1109/MSP.2020.2975749

[8] Lu, Y. (2025). The current status and developing trends of Industry 4.0: A review. Information Systems Frontiers, 27(1), 215-234. https://doi.org/10.1007/s10796-021-10221-w

[9] Bonawitz, K., Ivanov, V., Kreuter, B., Marcedone, A., McMahan, H. B., Patel, S., Ramage, D., Segal, A., & Seth, K. (2017). Practical secure aggregation for privacy-preserving machine learning. Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, 1175-1191. https://doi.org/10.1145/3133956.3133982

[10] Akter, S., Wamba, S. F., Gunasekaran, A., Dubey, R., & Childe, S. J. (2016). How to improve firm performance using big data analytics capability and business strategy alignment? International Journal of Production Economics, 182, 113-131. https://doi.org/10.1016/j.ijpe.2016.08.018

[11] Dwork, C., & Roth, A. (2014). The algorithmic foundations of differential privacy. Foundations and Trends in Theoretical Computer Science, 9(3-4), 211-407. https://doi.org/10.1561/0400000042

[12] Xu, L. D., Lu, Y., & Li, L. (2021). Embedding blockchain technology into IoT for security: A survey. IEEE Internet of Things Journal, 8(13), 10452-10473. https://doi.org/10.1109/JIOT.2021.3060508

[13] Wamba, S. F., Gunasekaran, A., Akter, S., Ren, S. J., Dubey, R., & Childe, S. J. (2017). Big data analytics and firm performance: Effects of dynamic capabilities. Journal of Business Research, 70, 356-365. https://doi.org/10.1016/j.jbusres.2016.08.009

[14] Mothukuri, V., Parizi, R. M., Pouriyeh, S., Huang, Y., Dehghantanha, A., & Srivastava, G. (2021). A survey on security and privacy of federated learning. Future Generation Computer Systems, 115, 619-640. https://doi.org/10.1016/j.future.2020.10.007

[15] Grover, V., Chiang, R. H. L., Liang, T. P., & Zhang, D. (2018). Creating strategic business value from big data analytics: A research framework. Journal of Management Information Systems, 35(2), 388-423. https://doi.org/10.1080/07421222.2018.1451951

[16] Wu, H. P., Liu, Z., Dong, H. Y., Lu, Y., & Xu, L. D. (2025). Revolutionizing internal auditing:

Harnessing the power of blockchain. Enterprise Information Systems, 19(1-2). https://doi.org/10.1080/17517575.2024.2448003

[17] Abadi, M., Chu, A., Goodfellow, I., McMahan, H. B., Mironov, I., Talwar, K., & Zhang, L. (2016). Deep learning with differential privacy. Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, 308-318. https://doi.org/10.1145/2976749.2978318

[18] Goldfarb, A., & Tucker, C. (2019). Digital economics. Journal of Economic Literature, 57(1), 3-43. https://doi.org/10.1257/jel.20171452

[19] Zheng, Y. (2015). Trajectory data mining: An overview. ACM Transactions on Intelligent Systems and Technology, 6(3), Article 29. https://doi.org/10.1145/2743025

[20] Chen, Y., Lu, Y., Bulysheva, L., & Kataev, M. Y. (2024). Applications of blockchain in Industry 4.0: A review. Information Systems Frontiers, 26(5), 1715-1729. https://doi.org/10.1007/s10796-022-10248-7

[21] Ivanov, D., & Dolgui, A. (2021). A digital supply chain twin for managing the disruption risks and resilience in the era of Industry 4.0. Production Planning & Control, 32(9), 775-788. https://doi.org/10.1080/09537287.2020.1768450

[22] Lim, W. Y. B., Luong, N. C., Hoang, D. T., Jiao, Y., Liang, Y. C., Yang, Q., Niyato, D., & Miao, C. (2020). Federated learning in mobile edge networks: A comprehensive survey. IEEE Communications Surveys & Tutorials, 22(3), 2031-2063. https://doi.org/10.1109/COMST.2020.2986024

[23] Rysman, M. (2009). The economics of two-sided markets. Journal of Economic Perspectives, 23(3), 125-143. https://doi.org/10.1257/jep.23.3.125

[24] Zhang, C., & Lu, Y. (2021). Study on artificial intelligence: The state of the art and future prospects. Journal of Industrial Information Integration, 23, 100224. https://doi.org/10.1016/j.jii.2021.100224

[25] Nguyen, D. C., Ding, M., Pathirana, P. N., Seneviratne, A., Li, J., Niyato, D., Dobre, O., & Poor, H. V. (2021). Federated learning for Internet of Things: A comprehensive survey. IEEE Communications Surveys & Tutorials, 23(3), 1622-1658. https://doi.org/10.1109/COMST.2021.3075439

[26] Gonzalez, M. C., Hidalgo, C. A., & Barabasi, A. L. (2008). Understanding individual human mobility patterns. Nature, 453(7196), 779-782. https://doi.org/10.1038/nature06958

[27] Dubey, R., Gunasekaran, A., Childe, S. J., Blome, C., & Papadopoulos, T. (2019). Big data and predictive analytics and manufacturing performance: Integrating institutional theory, resource-based view and big data culture. British Journal of Management, 30(2), 341-361. https://doi.org/10.1111/1467-8551.12355

[28] Lu, Y. (2019a). Artificial intelligence: A survey on evolution, models, applications and future trends. Journal of Management Analytics, 6(1), 1-29. https://doi.org/10.1080/23270012.2019.1570365

[29] Hagiu, A., & Wright, J. (2015). Multi-sided platforms. International Journal of Industrial Organization, 43, 162-174. https://doi.org/10.1016/j.ijindorg.2015.03.003

[30] Aledhari, M., Razzak, R., Parizi, R. M., & Saeed, F. (2020). Federated learning: A survey on enabling technologies, protocols, and applications. IEEE Access, 8, 140699-140725. https://doi.org/10.1109/ACCESS.2020.3013541

[31] Ben-Daya, M., Hassini, E., & Bahroun, Z. (2019). Internet of Things and supply chain management: A literature review. International Journal of Production Research, 57(15-16), 4719-4742. https://doi.org/10.1080/00207543.2017.1402140

[32] Lu, Y., & Yang, J. (2024). Quantum financing system: A survey on quantum algorithms, potential scenarios and open research issues. Journal of Industrial Information Integration, 41, 100663. https://doi.org/10.1016/j.jii.2024.100663

[33] Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. Organization Science, 10(1), 104-115. https://doi.org/10.1287/orsc.10.1.104

[34] Toorajipour, R., Sohrabpour, V., Nazarpour, A., Oghazi, P., & Fischl, M. (2021). Artificial intelligence in supply chain management: A systematic literature review. Journal of Business Research, 122, 502-517. https://doi.org/10.1016/j.jbusres.2020.09.009

[35] Shokri, R., & Shmatikov, V. (2015). Privacy-preserving deep learning. Proceedings of the 22nd ACM

SIGSAC Conference on Computer and Communications Security, 1310-1321. https://doi.org/10.1145/2810103.2813687

[36] Lu, Y. (2019b). The blockchain: State-of-the-art and research challenges. Journal of Industrial Information Integration, 15, 80-90. https://doi.org/10.1016/j.jii.2019.04.002

[37] Martin, K. D., & Murphy, P. E. (2017). The role of data privacy in marketing. Journal of the Academy of Marketing Science, 45(2), 135-155. https://doi.org/10.1007/s11747-016-0495-4

[38] Rochet, J. C., & Tirole, J. (2003). Platform competition in two-sided markets. Journal of the European Economic Association, 1(4), 990-1029. https://doi.org/10.1162/154247603322493212

[39] Lu, Y., & Xu, L. D. (2019). Internet of Things (IoT) cybersecurity research: A review of current research topics. IEEE Internet of Things Journal, 6(2), 2103-2115. https://doi.org/10.1109/JIOT.2018.2869847

[40] Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. Information Systems Research, 15(4), 336-355. https://doi.org/10.1287/isre.1040.0032

[41] Tiwana, A., Konsynski, B., & Bush, A. A. (2010). Platform evolution: Coevolution of platform architecture, governance, and environmental dynamics. Information Systems Research, 21(4), 675-687. https://doi.org/10.1287/isre.1100.0323

[42] Xu, R., Zhu, J., Yang, L., Lu, Y., & Xu, L. D. (2024). Decentralized finance (DeFi): A paradigm shift in the FinTech. Enterprise Information Systems, 18(9). https://doi.org/10.1080/17517575.2024.2397630

[43] Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. MIS Quarterly, 35(4), 989-1015. https://doi.org/10.2307/41409970

[44] Gunasekaran, A., Papadopoulos, T., Dubey, R., Wamba, S. F., Childe, S. J., Hazen, B., & Akter, S. (2017). Big data and predictive analytics for supply chain and organizational performance. Journal of Business Research, 70, 308-317. https://doi.org/10.1016/j.jbusres.2016.08.004

[45] Lu, Y. (2018). Blockchain and the related issues: A review of current research topics. Journal of Management Analytics, 5(4), 231-255. https://doi.org/10.1080/23270012.2018.1516523

[46] Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. Information Systems Research, 17(1), 61-80. https://doi.org/10.1287/isre.1060.0080

[47] Queiroz, M. M., Telles, R., & Bonilla, S. H. (2020). Blockchain and supply chain management integration: A systematic review of the literature. Supply Chain Management: An International Journal, 25(2), 241-254. https://doi.org/10.1108/SCM-03-2018-0143

[48] Xu, H., Dinev, T., Smith, H. J., & Hart, P. (2011). Information privacy concerns: Linking individual perceptions with institutional privacy assurances. Journal of the Association for Information Systems, 12(12), 798-824. https://doi.org/10.17705/1jais.00281

[49] Lu, Y. (2017a). Cyber physical system (CPS)-based Industry 4.0: A survey. Journal of Industrial Integration and Management, 2(3), 1750014. https://doi.org/10.1142/S2424862217500142

[50] Chen, H., Chiang, R. H. L., & Storey, V. C. (2012). Business intelligence and analytics: From big data to big impact. MIS Quarterly, 36(4), 1165-1188. https://doi.org/10.2307/41703503

[51] Lu, Y. (2017b). Industry 4.0: A survey on technologies, applications and open research issues. Journal of Industrial Information Integration, 6, 1-10. https://doi.org/10.1016/j.jii.2017.04.005

[52] Constantiou, I. D., & Kallinikos, J. (2015). New games, new rules: Big data and the changing context of strategy. Journal of Information Technology, 30(1), 44-57. https://doi.org/10.1057/jit.2014.17

[53] Yuan, J., Zheng, Y., Xie, X., & Sun, G. (2010). Driving with knowledge from the physical world. Proceedings of the 16th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 316-324. https://doi.org/10.1145/1835804.1835846

[54] Lu, Y., & Zheng, X. (2020). 6G: A survey on technologies, scenarios, challenges, and the related issues. Journal of Industrial Information Integration, 19, 100158. https://doi.org/10.1016/j.jii.2020.100158

[55] Günther, W. A., Mehrizi, M. H. R., Huysman, M., & Feldberg, F. (2017). Debating big data: A literature review on realizing value from big data. Journal of Strategic Information Systems, 26(3), 191-209. https://doi.org/10.1016/j.jsis.2017.07.003

[56] Lu, Y., & Ning, X. (2020). A vision of 6G-5G's successor. Journal of Management Analytics, 7(3), 301-

320. https://doi.org/10.1080/23270012.2020.1802622

[57] Huang, M. H., & Rust, R. T. (2021). A strategic framework for artificial intelligence in marketing. Journal of the Academy of Marketing Science, 49(1), 30-50. https://doi.org/10.1007/s11747-020-00749-9

[58] Zheng, X. R., & Lu, Y. (2022). Blockchain technology: Recent research and future trend. Enterprise Information Systems, 16(12), 1939895. https://doi.org/10.1080/17517575.2021.1939895

[59] Rieke, N., Hancox, J., Li, W., Milletari, F., Roth, H. R., Albarqouni, S., Bakas, S., Galtier, M. N., Landman, B. A., Maier-Hein, K., Ourselin, S., Sheller, M., Summers, R. M., Trask, A., Xu, D., Baust, M., & Cardoso, M. J. (2020). The future of digital health with federated learning. npj Digital Medicine, 3, Article 119. https://doi.org/10.1038/s41746-020-00323-1

[60] Lu, Y., Zheng, X., Li, L., & Xu, L. D. (2020). Pricing the cloud: A QoS-based auction approach. Enterprise Information Systems, 14(3), 334-351. https://doi.org/10.1080/17517575.2019.1669827

[61] Melis, L., Song, C., De Cristofaro, E., & Shmatikov, V. (2019). Exploiting unintended feature leakage in collaborative learning. Proceedings of the 2019 IEEE Symposium on Security and Privacy, 691-706. https://doi.org/10.1109/SP.2019.00029

[62] Ye, Z., & Lu, Y. (2022). Quantum science: A review and current research trends. Journal of Management Analytics, 9(3), 383-402. https://doi.org/10.1080/23270012.2022.2089064

[63] Martin, K. (2015). Privacy notices as tabula rasa: An empirical investigation into how complying with a privacy notice is related to meeting privacy expectations online. Journal of Public Policy & Marketing, 34(2), 210-227. https://doi.org/10.1509/jppm.14.139

[64] Lu, Y., Sigov, A. S., Ratkin, L., Ivanov, L. A., & Zuo, M. (2023). Quantum computing and industrial information integration: A review. Journal of Industrial Information Integration, 35, 100511. https://doi.org/10.1016/j.jii.2023.100511

[65] Kaissis, G. A., Makowski, M. R., Ruckert, D., & Braren, R. F. (2020). Secure, privacy-preserving and federated machine learning in medical imaging. Nature Machine Intelligence, 2(6), 305-311. https://doi.org/10.1038/s42256-020-0186-1

[66] Lu, W., Lu, Y., Li, J., Sigov, A., Ratkin, L., & Ivanov, L. A. (2024). Quantum machine learning: Classifications, challenges, and solutions. Journal of Industrial Information Integration, 42, 100736. https://doi.org/10.1016/j.jii.2024.100736

[67] Truong, N., Sun, K., Wang, S., Guitton, F., & Guo, Y. (2021). Privacy preservation in federated learning: An insightful survey from the GDPR perspective. Computers & Security, 110, 102402. https://doi.org/10.1016/j.cose.2021.102402

[68] Lu, Y., Ivanov, L. A., Wang, F., Pisarenko, Z. V., & Ye, C. (2024). Management analytics: A bibliometric analysis. Nanotechnologies in Construction, 16(3), 257-266. https://doi.org/10.15828/2075-8545-2024-16-3-257-266

[69] Huang, W., & Swaminathan, J. M. (2009). Introduction of a second channel: Implications for pricing and profits. European Journal of Operational Research, 194(1), 258-279. https://doi.org/10.1016/j.ejor.2007.11.041

[70] Lu, Y., Pisarenko, Z. V., Yang, L., & Ye, C. (2024). Advancing decision-making: The role of management analytics in modern business practices. Nanotechnologies in Construction, 16(5), 431-440. https://doi.org/10.15828/2075-8545-2024-16-5-431-440

[71] Belanger, F., & Crossler, R. E. (2011). Privacy in the digital age: A review of information privacy research in information systems. MIS Quarterly, 35(4), 1017-1042. https://doi.org/10.2307/41409971

[72] Kshetri, N. (2018). Blockchain's roles in meeting key supply chain management objectives. International Journal of Information Management, 39, 80-89. https://doi.org/10.1016/j.ijinfomgt.2017.12.005

[73] Lu, Y. (2021). Technological innovation and the emergence of a new interdisciplinary field: Management Analytics. Nanotechnologies in Construction, 13(3), 181-192. https://doi.org/10.15828/2075-8545-2021-13-3-181-192

[74] Ivanov, D. (2020). Predicting the impacts of epidemic outbreaks on global supply chains: A simulation-based analysis on the coronavirus outbreak. Transportation Research Part E: Logistics and Transportation Review, 136, 101922. https://doi.org/10.1016/j.tre.2020.101922

[75] Zhang, H., & Lu, Y. (2025). Web 3.0: Applications, opportunities and challenges in the next internet generation. Systems Research and Behavioral Science, 42(4), 996-1015. https://doi.org/10.1002/sres.3093

[76] McIntyre, D. P., & Srinivasan, A. (2017). Networks, platforms, and strategy: Emerging views and next steps. Strategic Management Journal, 38(1), 141-160. https://doi.org/10.1002/smj.2596

[77] Yuan, J., Zheng, Y., Xie, X., & Sun, G. (2011). Driving with knowledge from the physical world. ACM Transactions on Intelligent Systems and Technology, 3(1), Article 2. https://doi.org/10.1145/2036264.2036266

[78] Yang, L., Hou, Q., Zhu, X., Lu, Y., & Xu, L. D. (2025). Potential of large language models in blockchain-based supply chain finance. Enterprise Information Systems, 19(11), 2541199. https://doi.org/10.1080/17517575.2025.2541199

[79] Zuboff, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization. Journal of Information Technology, 30(1), 75-89. https://doi.org/10.1057/jit.2015.5

[80] Luca, M., Barlacchi, G., Lepri, B., & Pappalardo, L. (2021). A survey on deep learning for human mobility. ACM Computing Surveys, 55(1), Article 7. https://doi.org/10.1145/3485125