Personal Language Models, Federated Learning, and Brand Intelligence:

A Technical Blueprint for Privacy-Preserving, Consent-First Advertising

Intellex

May 1, 2025

Abstract

Large language models (LLMs) are becoming commoditized; the durable competitive moat shifts to *owned intelligence*: the personal or organizational knowledge that shapes an LLM's responses. This paper formalizes *Personal Language Models* (PLMs) as owner-controlled model specializations (via adapters, prompts, or fine-tunes) that encapsulate expertise, memory, preferences, and policies. We review the state of the art in *federated learning* (FL)—including secure aggregation and differential privacy—and design a practical protocol to *federate PLMs* for brand advertisers. We present algorithms and mathematical models (personalized FL objectives, federated contextual bandits, differentially private robust aggregation, and Shapley-style attribution) that quantify value while protecting privacy. Finally, we outline an implementable architecture, technical requirements, and an evaluation plan (lift, regret, and privacy-utility trade-offs).

1 Introduction

Traditional digital advertising relied on identifiers and centralized user profiles. Regulatory pressure and platform changes now constrain tracking. At the same time, powerful foundation models are widely available, which shifts advantage from "which LLM" a brand uses to *whose intelligence it runs on.* In this context, **Personal Language Models (PLMs)**—portable, permissioned specializations owned by individuals—offer a new way to conduct privacy-preserving research, creative testing, and measurement. Brands get aggregate, consented signals; people and organizations keep control of their intelligence.

Contributions. We: (i) define PLMs and situate them in current personalization research; (ii) summarize FL algorithms and privacy mechanisms relevant to PLM federation; (iii) formalize a *Federated PLM for Advertising* (FPLA) framework with mathematical objectives and algorithms; (iv) specify technical requirements and a reference architecture; and (v) sketch evaluation protocols for measuring advertising value (lift, ROI) under privacy constraints.

2 Personal Language Models (PLMs)

2.1 Definition

A PLM is an owner-controlled specialization of a base LLM that encapsulates a person's (or organization's) knowledge, preferences, and policies.

3 The Rise of Personal Language Models (PLMs)

Large language models (LLMs) are increasingly commoditized, which shifts the source of competitive advantage to the ownership and control of knowledge and behavioral data. Personal Language Models (PLMs) emerge as a mechanism to turn personal data and behavioral traces into intelligence assets that drive agents on behalf of individuals.

A PLM can be described as an owner-controlled specialization of a base model. Formally, a base LLM with frozen parameters ϕ is combined with user-specific lightweight parameters θ_u (adapters, LoRA, or prompt vectors), a retrieval memory $\mathcal{M}_u$ (documents, history, preferences), and a policy π_u that encodes consent rules. The PLM then computes:

$$\hat{y} = f(x; \phi, \theta_u, \mathcal{M}_u, \pi_u), \tag{1}$$

producing outputs that reflect the owner's intelligence without exposing raw data.

The conversion of personal data and behaviors into PLMs follows a pipeline: (i) ingestion and embedding of user-selected data sources (notes, documents, transactions, interactions); (ii) training of parameter-efficient adapters θ_u to encode task-specific preferences and expertise; (iii) application of policies π_u to govern who may query the PLM and under what scope; and (iv) optional participation in federated learning rounds, where only parameter updates are aggregated to improve a shared model without transferring sensitive data.

This trajectory positions PLMs as the foundation of personal agents. Agents powered by PLMs operate with memory, context, and policies that belong to their owners, enabling individuals to deploy their intelligence across apps, enterprises, and digital ecosystems without loss of sovereignty.

4 Valuing the Intelligence of Personal Language Models

Personal Language Models (PLMs) embody both *declarative intelligence* (facts, memory, knowledge) and *procedural intelligence* (skills, policies, decision rules). This echoes ACT–R, where declarative memory consists of chunks with activation that determines retrieval latency and probability, and procedural memory consists of productions with utilities that guide action selection [4].

4.1 Decision-Theoretic Value of Information

We can quantify intelligence by the *expected value of information* (VoI). If $U(a)$ is the utility of action a, then:

$$\mathrm{VoI} = \mathbb{E}\Big[\max_a \mathbb{E}[U(a) \mid \mathrm{info}]\Big] - \mathbb{E}\Big[\max_a \mathbb{E}[U(a)]\Big],$$

with EVPI/EVSI as special cases [15]. This captures how much better decisions are when a PLM is consulted.

4.2 Information-Theoretic Value

Declarative intelligence reduces uncertainty. For target Y, the information gain of a PLM is:

$$\Delta\mathrm{CE} = \mathbb{E}[-\log p_0(Y \mid X)] - \mathbb{E}[-\log p_{\mathrm{PLM}}(Y \mid X)],$$

equivalently the KL divergence between baseline and PLM-enhanced predictions [7]. This reduction in entropy can be monetized by mapping bits of improvement to ROI.

4.3 Procedural Value (Policy Improvement)

For action policies, the value is the uplift in expected return:

$$\Delta J = J(\pi_{\text{PLM}}) - J(\pi_0).$$

Off-policy evaluation methods such as doubly-robust estimators [9] allow unbiased estimates without deploying every policy live. This reflects the procedural competence of a PLM in guiding decisions.

4.4 Attribution and Contribution

When multiple PLMs contribute, value can be fairly allocated with Shapley values. Outcome-side Shapley assigns shares of conversion lift [25], while *Data Shapley* assigns value to data or federated updates [13, 24].

4.5 Productivity and ACT–R Grounding

ACT–R predicts retrieval time $T_i = Fe^{-A_i}$ where activation A_i reflects recency and frequency. A PLM that raises activation by ΔA yields expected time savings:

$$\Delta T \approx F\big(e^{-A} - e^{-(A+\Delta A)}\big).$$

The economic value is $v_{\text{minute}} \cdot \Delta T + v_{\text{error}} \cdot \Delta\text{Accuracy}$, where v_{minute} is time cost and v_{error} is the cost of an error.

4.6 Privacy and Risk Deduction

Valuation must account for privacy risk. Studies show willingness-to-pay and willingness-to-accept for privacy are highly context-dependent [2]. A risk deduction proportional to exposure (e.g., differential privacy ε) should be included.

4.7 Composite Value Score

We define a composite intelligence value score:

$$V_{\text{PLM}} = \alpha\Delta\text{CE} + \beta\text{VoI} + \gamma\Delta J + \delta\text{Shapley} + \eta\text{Prod\$} - \lambda\text{Risk},$$

where weights can be learned from historical ROI regressions or set by vertical norms.

5 The Economics of Consumer Engagement

Businesses spend heavily to influence consumer behavior—whether to build awareness, drive trial, or encourage repeat purchase. Understanding the scale and distribution of this spending provides context for the value of federated PLMs in advertising and shopper marketing.

5.1 Advertising Expenditure

Global advertising spend is projected to exceed 1 trillion USD by 2025, with GroupM estimating approximately 1.08 trillion and Magna forecasting around 979 billion depending on methodology. Growth rates are forecast in the range of 5–6% year-over-year, driven primarily by digital channels.

5.2 Shopper Marketing and Trade Promotion

Within consumer packaged goods (CPG), marketing expenditures go far beyond traditional advertising. In the U.S. alone, CPG marketing totals approximately 230 billion annually. Of this, nearly three-quarters flows through retailers, including trade promotion (∼48%), shopper marketing (∼13%), and retail media (∼12%). This reflects the emphasis on shaping behavior at the point of purchase, rather than only raising awareness.

5.3 Retail Media

Retail media, the practice of serving ads within retailer-owned digital platforms, is the fastest growing segment, valued at more than 155 billion in 2024 and expected to continue double-digit growth. This shift reflects the value of proximity to purchase decisions and the ability to attribute outcomes.

5.4 Direct Incentives

Coupons, loyalty programs, and promotions are additional major instruments for shaping consumer behavior. U.S. coupon distribution remains large—tens of billions annually—though increasingly digital-first. Loyalty program software alone represents a market of more than 12 billion, growing rapidly with consumer adoption.

5.5 Implication for PLMs

Advertising, shopper marketing, and promotional spending are all essentially attempts to predict, measure, and influence behavior. PLMs federated under privacy-preserving protocols offer a mechanism for brands to query consumer intelligence directly, with consent, to optimize creatives, offers, and attribution. This re-anchors the economics of engagement away from identifiers and tracking, and toward federated intelligence markets that respect ownership of memory.

5.6 Parameter-efficient personalization

Modern personalization favors parameter-efficient fine-tuning (PEFT): prompt/soft-prompt tuning, adapters, and low-rank adaptation (LoRA). Let θ_u be low-dimensional (rank-r updates) so that PLMs are lightweight, portable, and easy to federate. Retrieval-augmented generation (RAG) adds $\mathcal{M}_u$ without modifying ϕ.

5.7 Privacy, provenance, and consent

A PLM must bind identity (keys), provenance (where knowledge came from), and consent (π_u). We model *licenses* as tokens that grant scoped access: $\ell = \langle \text{asset\_id}, \text{scope}, \text{cap}, \text{expiry} \rangle$. Every query produces a signed receipt (r, σ) and updates counters for metering and budgeting.

6 Federated Learning (FL): Status and Trajectory

6.1 Core optimization

In cross-device FL, clients minimize the global risk without sharing raw data:

$$\min_{\phi} \; F(\phi) := \sum_{u=1}^{U} p_u \; \underbrace{\mathbb{E}_{(x,y)\sim\mathcal{D}_u}\left[\ell(f(x;\phi), y)\right]}_{=:\; f_u(\phi)}, \tag{2}$$

with $p_u \propto |\mathcal{D}_u|$. FedAvg computes local steps on clients and averages parameters or gradients:

$$\phi_u^{t+1} \leftarrow \phi^t - \eta \nabla f_u(\phi^t) \quad \text{(local } E \text{ epochs)}, \tag{3}$$

$$\phi^{t+1} \leftarrow \sum_{u \in \mathcal{S}_t} w_u \phi_u^{t+1}, \quad w_u = \frac{|\mathcal{D}_u|}{\sum_{j \in \mathcal{S}_t} |\mathcal{D}_j|}. \tag{4}$$

FedProx stabilizes training under heterogeneity by adding a proximal term to the local objective:

$$\min_{\phi} \sum_u p_u \min_{\Delta} \; f_u(\phi + \Delta) + \frac{\mu}{2} \|\Delta\|^2. \tag{5}$$

Personalized FL (PFL) seeks client-specific models ϕ_u while sharing a global representation ϕ; e.g., Per-FedAvg or proximal regularization toward ϕ.

6.2 Secure aggregation and differential privacy

To protect updates, clients send masked gradients for *secure aggregation*; the server sees only the sum. Differentially private SGD (DP-SGD) clips per-client gradients and adds noise calibrated by (ε, δ), tracked by a moments/Bayesian/Wasserstein accountant. In production, *participation* and *sampling* policies also impact the privacy-utility trade-off.

6.3 PLM-ready FL

For PLMs, communication-compressed updates (adapters/LoRA) reduce bandwidth; *federated adapters* aggregate only θ-blocks while keeping ϕ frozen. Retrieval memories $\mathcal{M}_u$ are never transmitted; only derived updates or statistics move.

7 Federating PLMs for Brand Advertisers

7.1 Problem setting

A brand b wants to estimate preference or intent for creative variants $v \in \mathcal{V}$ from a population of owners $\mathcal{U}$. Each PLM u returns a score $s_{uv} \in [0, 1]$ and optional rationale z_{uv} under license ℓ. The coordinator aggregates $\{s_{uv}\}$ with privacy, consent, and budget constraints to deliver segment-level insights and to conduct small-scale experiments.

7.2 Aggregation with privacy and robustness

Let α_u be a trust/reputation weight (attestations, payment history). We output a DP-protected, robust mean per variant:

$$\tilde{m}_v = \mathrm{MOM}\left(\{\alpha_u s_{uv}\}_{u \in \mathcal{U}_v}\right) + \mathcal{N}(0, \sigma_v^2), \tag{6}$$

where MOM is a median-of-means estimator, and σ_v is set by the privacy budget (ε, δ) and sensitivity (bounded by clipping). Confidence intervals reflect both sampling and DP noise.

7.3 Federated contextual bandits for creative testing

We model creative selection as a federated contextual bandit. For user u with context x_u and creative features ϕ_v, assume linear reward $r_{uv} = x_u^\top \beta_v + \epsilon$. Fed-LinUCB maintains global $\hat{\beta}_v$ via secure aggregation of local sufficient statistics:

$$A_v = \lambda I + \sum_u x_u x_u^\top, \quad b_v = \sum_u x_u r_{uv}, \quad \hat{\beta}_v = A_v^{-1} b_v. \tag{7}$$

Each PLM proposes $v^* = \arg\max_v x_u^\top \hat{\beta}_v + \alpha \sqrt{x_u^\top A_v^{-1} x_u}$, logs local outcomes (simulated or real), and contributes differentially-private updates to (A_v, b_v).

7.4 Attribution and value

Let y be conversion. Compare a global model $p(y|x)$ to a PLM-personalized model $p(y|x,u)$. The *value of personalization* is

$$\Delta_{\text{VoI}} = \mathbb{E}\left[\log p(y|x,u)\right] - \mathbb{E}\left[\log p(y|x)\right]. \tag{8}$$

Campaign credit can be divided with Shapley values over features (creative, channel, audience) computed from counterfactual loss reductions; privacy-preserving approximations (weighted/approximate Shapley) scale to federated settings.

8 Algorithms

8.1 Personalized FL objective with adapters

Let ϕ be frozen and θ_u be user adapters. We solve

$$\min_{\phi,\{\theta_u\}} \sum_u p_u \, \mathbb{E}_{(x,y)\sim\mathcal{D}_u}\big[\ell(f(x;\phi,\theta_u),y)\big] + \lambda\|\theta_u\|_2^2. \tag{9}$$

Two-time-scale updates: periodically update ϕ by aggregating adapter gradients or by meta-learning (Per-FedAvg); update θ_u locally between rounds.

8.2 Secure aggregation protocol (sketch)

Each client samples masks $m_{u\to v}$ for peers, sends $(g_u + \sum_v m_{v\to u} - \sum_v m_{u\to v})$; masks cancel in sum $\sum_u g_u$. Dropout-robust variants use pairwise keys and secret sharing.

8.3 DP-SGD (client level)

Clip local update $g_u \leftarrow g_u \cdot \min\left(1, \frac{C}{\|g_u\|}\right)$ and add noise: $\tilde{g}_u = g_u + \mathcal{N}(0, \sigma^2 C^2 I)$. The server aggregates $\tilde{g}_u$; the privacy accountant tracks the total (ε, δ) over rounds.

8.4 Federated LinUCB (coordinator-side)

Algorithm 1: Federated LinUCB for Creative Selection

Input: Contexts $\{x_u\}$, creative features $\{\phi_v\}$, regularizer λ, exploration α

Initialize $A_v \leftarrow \lambda I,\ b_v \leftarrow 0$ for all v

for *round* $t = 1, 2, \ldots$ **do**

- Each client u receives $\{\hat{\beta}_v = A_v^{-1} b_v\}$
- Client selects $v_u \leftarrow \arg\max_v x_u^\top \hat{\beta}_v + \alpha\sqrt{x_u^\top A_v^{-1} x_u}$
- Observe reward r_{uv_u} (e.g., click/like/purchase or simulated feedback)
- Form local stats $A_{v_u}^{(u)} \leftarrow x_u x_u^\top,\ b_{v_u}^{(u)} \leftarrow x_u r_{uv_u}$
- Apply DP noise to $A_{v_u}^{(u)}, b_{v_u}^{(u)}$ and send via secure aggregation
- Server updates $A_{v_u} \leftarrow A_{v_u} + \sum_u A_{v_u}^{(u)}$ and $b_{v_u} \leftarrow b_{v_u} + \sum_u b_{v_u}^{(u)}$

9 System Requirements and Architecture

Owner layer. Key management (wallet or hardware enclave), PLM container (hosts θ_u and $\mathcal{M}_u$), consent/policy UI, local logging.

Coordinator layer. **(i)** *Registry* for PLMs/licenses; **(ii)** *Gateway* API for scoped queries; **(iii)** *Aggregation service* implementing secure aggregation, DP accounting, robust estimators; **(iv)** *Experiment service* (federated bandits, A/B); **(v)** *Settlement* for micro-royalties and refunds; **(vi)** *Audit* and provenance explorer.

Privacy & safety. Client-level DP, secure aggregation, rate limiting, content safety filters, license caps, revocation with "tombstones" and propagation SLAs.

Brand interfaces. Creative upload, question templates, budget and privacy knobs (max ε, min cohort size), dashboards for lift/attribution with confidence intervals.

10 Value for Brand Advertisers

Audience understanding without identifiers. PLMs provide preference signals aggregated with DP; brands get statistically sound answers while owners retain control. **Creative/search cost reduction.** Federated bandits lower exploration cost by sharing learning across PLMs without moving raw data. **Faster iteration.** Scoped licenses and instant receipts enable near-real-time research with built-in compliance evidence. **Attribution that survives privacy changes.** Shapley-style contributions computed from counterfactual loss reductions can be reported within DP budgets.

11 Evaluation Plan

Offline: replay logs or synthetic user simulators to measure Δ_{VoI}, CTR lift, regret of Fed-LinUCB, privacy-utility trade-offs for different (ε, δ). Online: limited-scope pilots with pre-registered analysis, holdouts, and DP-bounded reporting. Robustness: Byzantine client tests with trimmed-mean/Krum aggregators; fairness: group constraints in bandit optimization.

12 Limitations and Outlook

PLMs can embed bias; DP noise reduces sensitivity but also utility; secure aggregation adds system complexity. Future work: cross-model routing with cost/provenance constraints; adapter marketplaces; cryptographic enforcement of license revocation; incentive alignment for contribution quality.

13 Conclusion

Federating PLMs reframes brand intelligence from data collection to *consented computation at the edge*. With modern FL (secure aggregation, DP), robust estimation, and bandit-style experimentation, brands can learn "what works" while individuals keep control. The math and system components presented here provide a practical path to deploy such a platform today.

References

[1] M. Abadi et al., "Deep Learning with Differential Privacy," CCS, 2016. `https://arxiv.org/abs/1607.00133`.

[2] Acquisti, A., John, L., & Loewenstein, G. *What Is Privacy Worth?*. J. Legal Studies, 2013.

[3] J. Pfeiffer et al., "AdapterFusion: Non-destructive Task Composition for Transfer Learning," EACL, 2021. https://aclanthology.org/2021.eacl-main.39/.

[4] Anderson, J.R. et al. *An Integrated Theory of the Mind*. Psychological Review, 2004.

[5] K. Bonawitz et al., "Practical Secure Aggregation for Privacy-Preserving Machine Learning," CCS, 2017. https://arxiv.org/abs/1611.04482.

[6] Chen et al., "Personalized Federated Learning via Feature Distribution Adaptation (pFedFDA)," NeurIPS, 2024. https://papers.nips.cc/paper_files/paper/2024/file/8ce6c5450ccddbe6adee4b3749893587-Paper-Conference.pdf.

[7] Cover, T.M. & Thomas, J.A. *Elements of Information Theory*. Wiley, 2006.

[8] Dinh et al., "Personalized Federated Learning with Moreau Envelopes (pFedMe)," NeurIPS, 2020. https://proceedings.neurips.cc/paper/2020/hash/f4f1f13c8289ac1b1ee0ff176b56fc60-Abstract.html.

[9] Dudík, M. et al. *Doubly Robust Policy Evaluation and Learning*. ICML, 2011.

[10] A. Fallah et al., "Personalized Federated Learning: A Meta-Learning Approach (PerFedAvg)," NeurIPS, 2020. https://arxiv.org/abs/2002.07948.

[11] T. Li, A. K. Sahu, et al., "Federated Optimization in Heterogeneous Networks (FedProx)," MLSys, 2020. https://arxiv.org/abs/1812.06127.

[12] Google Research Blog, "Improving Gboard via Private Federated Analytics," 2024. https://research.google/blog/improving-gboard-language-models-via-private-federated-analytics/.

[13] Ghorbani, A. & Zou, J. *Data Shapley: Equitable Valuation of Data for Machine Learning*. ICML, 2019.

[14] Google Research, "Federated Learning of Gboard Language Models with Differential Privacy," 2023. https://research.google/pubs/federated-learning-of-gboard-language-models-with-differential-privacy/.

[15] Howard, R.A. *Information Value Theory*. IEEE Transactions on Systems Science and Cybernetics, 1966.

[16] P. Kairouz et al., "Advances and Open Problems in Federated Learning," FnT ML, 2021. https://www.nowpublishers.com/article/Details/MAL-083.

[17] L. Li et al., "A Contextual-Bandit Approach to Personalized News Article Recommendation," WWW, 2010. https://arxiv.org/abs/1003.0146.

[18] J. Liu et al., "A Survey of Personalized Large Language Models," 2025. https://arxiv.org/abs/2502.11528.

[19] E. Hu et al., "LoRA: Low-Rank Adaptation of Large Language Models," 2021. https://arxiv.org/abs/2106.09685.

[20] H. B. McMahan et al., "Communication-Efficient Learning of Deep Networks from Decentralized Data," AISTATS, 2017. https://arxiv.org/abs/1602.05629.

[21] B. Lester et al., "The Power of Scale for Parameter-Efficient Prompt Tuning," 2021. https://arxiv.org/abs/2104.08691.

[22] PETS, "Differentially Private Ad Conversion Measurement," 2024. https://petsymposium.org/popets/2024/popets-2024-0044.pdf.

[23] Zhao et al., "Shapley Value Methods for Attribution Modeling in Online Advertising," 2018. https://arxiv.org/abs/1804.05327.

[24] Wang, T. et al. *A Principled Approach to Data Valuation for Federated Learning*. ICML, 2020.

[25] Zhao, X. et al. *Shapley Value Methods for Attribution Modeling in Online Advertising*. 2018.