



# Worldwide Federated Training of Language Models

Ilex Iacob<sup>1,2</sup>

Lorenzo Sani<sup>1,2</sup>

Bill Marino<sup>1</sup>

Preslav Ieksandrov<sup>1</sup>

William F. Shen<sup>1</sup>

Nicholas D. Lane<sup>1,2</sup>

## Abstract

The reliance of language model training on massive amounts of computation and vast datasets scraped from potentially low-quality, copyrighted, or sensitive data has come into question practically, legally, and ethically. Federated learning provides a plausible alternative by enabling previously untapped data to be voluntarily gathered from collaborating organizations. However, when scaled globally, federated learning requires collaboration across heterogeneous legal, security, and privacy regimes while accounting for the inherent locality of language data; this further exacerbates the established challenge of federated statistical heterogeneity. We propose a Worldwide Federated Language Model Training (*WorldLM*) system based on **federations of federations**, where each federation has the autonomy to account for factors such as its industry, operating jurisdiction, or competitive environment. *WorldLM* enables such autonomy in the presence of statistical heterogeneity via partial model localization by allowing sub-federations to attentively aggregate key layers from their constituents. Furthermore, it can adaptively share information across federations via residual layer embeddings. Evaluations of language modeling on naturally heterogeneous datasets show that *WorldLM* outperforms standard federations by up to  $1.91\times$ , approaches the personalized performance of fully local models, and maintains these advantages under privacy-enhancing techniques.

## 1 Introduction

Contemporary Language Models (LMs) are trained in data centers with numerous hardware accelerators [61, 50] on large scraped corpora [9, 42]. This paradigm has restricted training to well-funded actors and brought concerns regarding centralization [5, sec. 4.7.1], copyright [22], and the limited supply of data [70]. While small organizations may own valuable data, the per-batch synchronization constraints of stochastic gradient descent (SGD) [56, 84] make collaboration impractical. Federated Learning (FL) has been proposed as an alternative [13, 75, 59] due to its lower synchronization constraints, limited data movement, and ability to integrate privacy-enhancing techniques [72, 6].

This work addresses the novel challenges that global-scale FL applications face. The first challenge is related to **federated governance** [21]: how to create federated systems including participants with different legal, privacy, and security concerns or combine existing systems seamlessly without

<sup>1</sup>Department of Computer Science and Technology, University of Cambridge

<sup>2</sup>Flower Labs

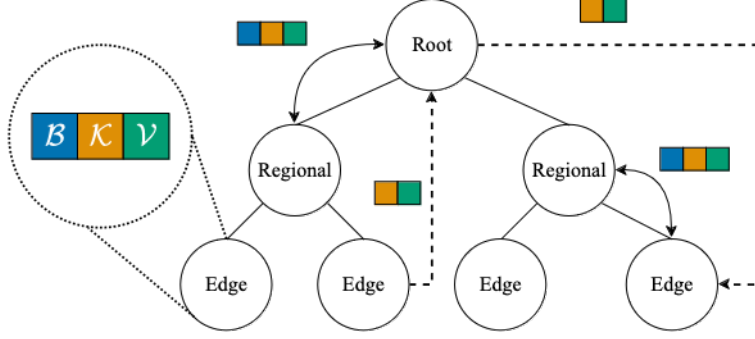


Figure 1: *WorldLM* federations exchange information in the form of models containing a backbone, personalized layers ( $\mathcal{B}, \mathcal{K}, \mathcal{V}$ ), and lower-dimensional residual embeddings serving as keys and values ( $\mathcal{K}, \mathcal{V}$ ). While full models are exchanged between parents and children, residuals are dynamically routed to the most appropriate sub-federation to be used in attention-based aggregation.

sacrificing performance. The second challenge is the **statistical heterogeneity** of naturally distributed data, as organizations may have datasets that differ in terms of language (e.g., for federations spanning multiple countries) and genres (e.g., publishers operating in different domains). Significant heterogeneity has been shown to slow model convergence or even cause divergence in standard single-federation settings [33, 85, 81]. This issue is worsened at a global level, as external factors [16] can implicitly create different clusters of data in the federation, making it necessary to optimize a participant’s parameters with respect to both the global distribution and its peers.

Our proposed Worldwide Federated Language Model (*WorldLM*) training system addresses both challenges by building **federations of federations**, as seen in Fig. 1. This brings several advantages:

1. **Arbitrary Federation Structure:** *WorldLM* allows each federation to adapt to its unique legal, privacy, and security requirements and also permits easy integration between previously isolated organizations, with differential privacy [72] protocols.
2. **Partially-personalized aggregation:** *WorldLM* takes advantage of cluster relationships within federations by segmenting models into a *backbone* serving as a shared feature extractor trained using standard FL algorithms [48] and partially-personalized *key* layers relevant to a node. These *key* layers are aggregated using attention over the keys of its peers. Results show that the aggregation procedure of *WorldLM* allows it to achieve a perplexity lower by 11.5-45.3% on a novel hierarchical partitioning of *The Pile* [18] dataset (e.g, Fig. 2) and on a language-partitioned *mC4* dataset [80]. Furthermore, *WorldLM* converges to similar performance when using differential privacy, whilst standard FL diverges completely.
3. **Cross-federation Information Sharing:** To address intra-federation heterogeneity, where a participant may contain data that is more similar to another sub-federation than to its peers, *WorldLM* can route *residual* parameters to the most relevant sub-federation in a communication-efficient fashion based on *key* similarity. Including such residuals allows *WorldLM* to partially maintain performance even when the underlying sub-federations contain dissimilar participants while requiring the transfer of a limited number of additional transformer blocks. We find the last 1 – 3 blocks to be sufficient.

The novel optimization algorithm and residual information routing of *WorldLM* tackle the challenges of global LM training without diverging far from the infrastructure of production systems [7]. Thus, it provides an effective solution for training LMs across legal, socioeconomic, and cultural boundaries, diversifying the pool of available data away from its current geographic [16] concentration.

## 2 Background

Well-known performance scaling laws [34, 24] drive LM training. The resulting models [61, 66, 67, 50] have led to numerous decentralized downstream applications [25, 45, 4, 19, 78]. However, since the Ring AllReduce algorithm [62] used to synchronize the model state for every batch [56, 84] requires high cross-GPU bandwidth, pre-training still requires large centralized datacenters [50].

Douillard et al. [13] relax the communication requirements of training via Local SGD [65], a data-parallel technique synchronizing independent model replicas. Based on the observation that publically available data may not keep up with the demands of LM training [70], future work [59] extended generative pre-training to Federated Learning (FL) settings and showed performance comparable to centralized training even for billion-scale models. This shift enables collaboration across geographically distributed actors with valuable data currently serving as passive data providers [53, 54]. Given the potential of FL to reach untapped data reservoirs, we are motivated by these results to tackle the challenges that emerge when applied at a *global* scale.

## 2.1 Global Federated Systems

Standard federated training proceeds in rounds that involve broadcasting a shared set of parameters to all clients, local optimization of said parameters on private data, and then aggregation [48]. Its roots in the principle of data minimization [48, 73] make FL an attractive paradigm across international regulatory frameworks [74, 75] (Appendix A.1). However, while it is communication-efficient and scalable, FL suffers from **statistical** and **system** heterogeneity, defined as clients having different data distributions, training speeds, or communication bandwidth. For example, Charles et al. [10] and Zhou et al. [85] observe that training on more clients within a round brings diminishing returns due to near-orthogonal updates. These behaviors are analogous to the limitations of large-batch training [35], indicating the need for more sophisticated aggregation strategies, unlike the Local SGD literature [40], which assumes homogeneous data. Similarly, systems heterogeneity can result in varying client completion times [7, 27], causing stragglers and slow convergence.

Since high-quality language data is liable to run out within the decade [70], the quality of data that FL makes available is also paramount. For example, obtaining data from regions with a reduced internet presence may alleviate the challenges associated with low-resource languages [46, 57]. We argue that the impact of data and systems heterogeneity increases as the reach of the federated system grows, which causes governance to emerge as a new challenge.

Federated governance, hitherto considered primarily in the medical domain [55, 63], requires determining how to create systems spanning actors with different legal, privacy, and security concerns and how to combine already existing federations. For example, unlike US-based organizations, training an LM on the private data of EU-based organizations requires abiding by the GDPR [15], which restricts cross-border data transfer, while mitigating bias [12, Art. 10.2f,fa] (see Appendix A.1). Although differential privacy (DP) [72] or secure aggregation [6] may enable collaboration across legally heterogeneous regions, not using them within a region when possible avoids computational and performance costs [6, 64, 32, 49]. Similar hierarchical structures enable collaboration in platform ecosystems [68, 36], OSS [30], and vertical FL on medical data [31, sec. 2.4.1].

Privacy-enhancement techniques (PETs), such as DP [14] or secure aggregation, have become popular in FL since client updates may leak private information [79]. Researchers and practitioners consider DP the de facto method for alleviating privacy concerns in FL [72, 33], as it provides statistical bounds on the leakage of private information.

## 2.2 Related Work

Previous works in standard federated learning have tackled aspects of data and systems heterogeneity relevant to our work [38, 33, 82, 81]. However, they are unable to account for the complexities of building federations-of-federations. Personalized Federated Learning (PFL) [44] attempts to tackle the performance disparity between clients induced by the heterogeneity of client data by creating personalized models. The most common means of achieving this is a local adaptation (fine-tuning) of the federated model after training [82, 47, 11, 11]. Split approaches such as those of Arivazhagan et al. [3] and Li et al. [39] train models locally but only average and update the layers up to a cut layer  $q$ , with the intuition that earlier layers represent feature extractors.

Another means of tackling data heterogeneity is clustering clients based on a similarity metric between the flattened model embeddings [20, 60, 8, 26]. However, such approaches reduce the compatibility of client models to a single scalar and do not consider the structure of the model. Clusters may also exist naturally based on characteristics like location or language, which become relevant if the clients and servers controlling them are geographically correlated. However, most previous works in this

area have focused solely on communication efficiency rather than data heterogeneity [41, 1, 43, 71]. As such, they broadcast a global model rather than server personalization.

Mhaisen et al. [51] do consider scenarios where the data distribution of edge servers is taken into account and propose optimal user-edge assignment. While promising, their work assumes that edge servers have sufficiently low communication latency to efficiently train with FedSGD despite the original work of McMahan et al. [48] showing FedSGD to be up to two orders of magnitude slower than FedAvg in terms of convergence speed. Another work that addresses data heterogeneity within hierarchical FL is Wu et al. [77]; however, their framework focuses on well-known client-level fine-tuning strategies and never explicitly utilizes the hierarchical structure to enhance personalization.

### 3 World M

Given the interlocking nature of legal, privacy, and security concerns, we assume that organizations find it easier to collaborate with enterprises operating in the same geographic region, legal jurisdiction, or industry. Therefore, a key design objective for our system is facilitating these types of collaborations. In edge-device FL, the large number of potentially ephemeral participants with fine-grained preferences leads to a fully decentralized collaborative learning paradigm [33, 83] where the server-client federated network is replaced by a graph encoding client compatibility. For training LMs, where the participating entities are stable organizations, we argue that a **federation of federations** approach, as portrayed in Fig. 1, provides an attractive compromise between standard federated learning and decentralized learning. To optimize in this setting, *WorldLM* takes advantage of a custom aggregation procedure and information-sharing mechanism.

#### 3.1 Partially-personalized aggregation

---

**Algorithm 1** Fit: execution procedure for a given sub-federation.

---

**Require:** Node id  $q$ , parent backbone  $\mathcal{B}_p$ , sequence of key layers  $\mathcal{K}_p$

**Require:** Downstream residuals for aggregation  $\mathcal{D}_a$  for routing  $\mathcal{D}_r^0$

---

```

1:  $\mathcal{B}^0, \mathcal{K}^0 \leftarrow \text{LoadModel}(q)$ 
2:  $\mathcal{U}^0 \leftarrow \emptyset$  Upstream residuals for parent
3: if  $q \neq 0$  then If the current node is not root
4:    $\mathcal{Q}, \mathcal{K}, \mathcal{V} \leftarrow \mathcal{K}^0, [\mathcal{K}^0, \mathcal{K}_p, \mathcal{D}_a], [\mathcal{K}^0, \mathcal{K}_p, \mathcal{D}_a]$ 
5:    $\mathcal{B}^0 \leftarrow \mathcal{B}_p$ 
6:    $\mathcal{K}^0 \leftarrow \text{Attn}(\mathcal{Q}, \mathcal{K}, \mathcal{V})$  Agg. node, parent and residual key layers
7: for round  $k \leftarrow 0, \dots, K-1$  do
8:    $A^k, R^k \leftarrow \text{RouteResiduals}(\mathcal{D}_r^k, C)$  Route using similarity to cached children  $\mathcal{K}$ 
9:    $\text{Train}(q, \mathcal{B}^k, \mathcal{K}^k)$  Train node params sequentially or in-parallel
10:  for child  $c \in C_q$  do In parallel
11:     $\mathcal{B}_c^k, \mathcal{K}_c^k, \mathcal{U}_c^k \leftarrow \text{Fit}(c, \mathcal{B}^k, \mathcal{K}^k, A_c^k, R_c^k)$   $\mathcal{U}_c^k$  are residuals sent upstream by the child
12:     $\mathcal{B}_c^k \leftarrow \mathcal{B}_c^k \cup \mathcal{B}$  Compute backbone pseudo-gradient
13:  if  $C_q \neq \emptyset$  then
14:     $\mathcal{B}^{k+1} \leftarrow \frac{1}{|C_q|} \sum_{c \in C_q} \mathcal{B}_c^k$  Aggregate pseudo-gradients
15:     $\mathcal{B}^{k+1} \leftarrow \text{ServerOpt}(\mathcal{B}^{k+1}, \mathcal{K}^k, k)$  Apply pseudo-gradient
16:     $\mathcal{Q}, \mathcal{K}, \mathcal{V} \leftarrow [\mathcal{K}_0^k, \dots, \mathcal{K}_{|C_q|-1}^k], \dots, [\mathcal{K}_0^k, \dots, \mathcal{K}_{|C_q|-1}^k]$  Pack key layers with the same index
17:     $\mathcal{K}^{k+1} \leftarrow \text{Attn}(\mathcal{Q}, \mathcal{K}, \mathcal{V})$ 
18:     $\mathcal{U}^{k+1}, \mathcal{D}_r^{k+1} \leftarrow \text{PartitionResiduals}(q, \mathcal{K}^{k+1}, \mathcal{V}, \mathcal{U}^k, \mathcal{D}_r^k)$  Based on dissimilarity
return  $\mathcal{B}^k, \mathcal{K}^k, \mathcal{U}^k$ 

```

---

Federated learning can train powerful feature extractors beneficial to all *WorldLM* participants due to its meta-learning properties[52, 17, 37]. However, actors in the federated training process may

hold heterogeneous data; for example, it may be in a different language or come from a separate domain (e.g., one organization may publish news while another focuses on scientific publications). Thus, the feature extractor needs to be adapted to the data of each actor and sub-federation, which requires a departure from the standard FL objective. Thus, *WorldLM* takes inspiration from split-learning techniques [3, 39] and partitions the model into a backbone  $\mathcal{B}$ , comprising the majority of the model’s parameters, and a set of partially personalized key layers  $\mathcal{K}$  specific to each node. In practice, we expect the key layers to include the final 1-3 transformer blocks.

The backbone parameters  $\mathcal{B}$  are trained using FL aggregation algorithms such as FedAvg [48] or FedOPT [58]. As shown in Algorithm 1 (L.8–12), for each round  $k$ , the server broadcasts  $\mathcal{B}$  to its children  $c \in C_q$ . When a child begins execution, it replaces its previous backbone with the one received from the parent (L.5), and then executes its own sub-federation (L.10–12) and/or local training (L.9) and computes pseudo-gradients  $\nabla_c^k$ . These pseudo-gradients are then aggregated and applied to the backbone of the server via ServerOpt (L.15). It is important to note that local training (L.9) can be executed either **in-parallel** with the node model treated as a client or **sequentially**. Similarly, when observing the performance of a hierarchical FL approach we distinguish between sequential and parallel steps as parallel steps are averaged across clients. For this work, we choose the **sequential** approach, meaning that for the first level of the hierarchy, the root executes by itself, whilst for the final level, all leaves are executing **simultaneously**.

Unlike traditional personalization approaches, *WorldLM* optimizes the key layers  $\mathcal{K}$  while considering the models of its parent and children. It achieves this by aggregating each layer within  $\mathcal{K}$  using an attention mechanism [69, 29] where the parameters of that given layer across the nodes of the federation represent the queries, keys, and values. To exploit the locality of data and the similarity of nodes within the same sub-federation, the attention mechanism is applied within a local context, either with respect to the parent of a given node or its children. This procedure allows *WorldLM* to handle statistical heterogeneity when the nodes within a sub-federation have a similar data distribution.

### 3.2 Cross-Federation Information Sharing

The attention-based aggregation of a node’s children (L.17) will reduce to simple unweighted averaging when a cluster relationship does not exist in a sub-federation. In contrast, the aggregation between a node and its parent (L.6) will focus almost exclusively on the keys of the node and thus approach a personalization-layer strategy. Similarly, if a given node has a data distribution that differs significantly from its peers, its key layers will be highly dissimilar and ignored in the aggregation.

However, being dissimilar to its peers does not preclude a node from containing valuable data for another sub-federation. Inspired by residual connections [23], we introduce the concept of residual key layers, which are dynamically chosen based on their dissimilarity to peers and routed to a more appropriate sub-federation. For each layer of its post-aggregation key  $\mathcal{K}$ , a node selects at most  $\kappa$  of its children’s layers with the lowest similarity score (L.18), e.g., by the dot product. It then sends these residual layer embeddings to the highest permissible level of the federation as dictated by the participants’ legal, security, and privacy concerns. This server then routes the residuals to its highest-similarity children based on a cached set of keys from the previous round (L.8) by placing them in  $R^k$ . When the residuals reach an edge node, they are placed in  $A^k$  and later aggregated. Aggregating in the edge nodes (L.4–6) has the benefit of diffusing information into the entire sub-federation right after local training.

## 4 Experimental Design

Given the recent emergence of federated generative pre-training and the lack of benchmark datasets, we evaluate *WorldLM* on tasks that approximate realistic scenarios for its application: (a) organizations in different industries collaborating to train an LM despite holding different genres of text, (b) organizations trying to train an LM despite holding data in different languages.

To simulate organizations holding different genres of text, we partition *The Pile* [18] into its constituent heterogeneous datasets and construct federations of federations by bottom-up building different mixtures of datasets. For example, as seen in Fig. 2, if the children of a node hold data from

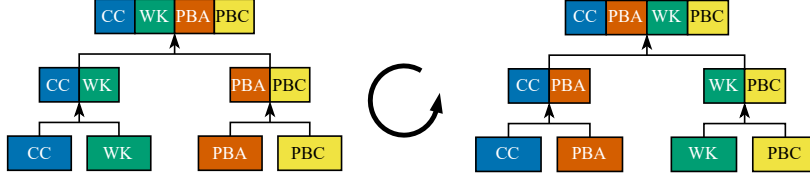


Figure 2: Data-perspective upon a hierarchical dataset constructed from The Pile [18]. The LHS contains two naturally heterogeneous and quantity-skewed groupings of data sources, corresponding to organizations accessing data from the internet or the medical domain. We construct such groupings using the internet-based Common Crawl (CC) and Wikipedia (WK) versus the medical data of PubMed Abstracts (PBA) and PubMed Central (PBC). To test the effectiveness of *WorldLM* when such a cluster relationship is absent, we swap the position of the two smaller datasets.

Table 1: Hyperparameters for *WorldLM*, the federated learning rate  $\eta_s$  and momentum  $\mu_s$  [28] are applied by a standard FL server or **each** server of *WorldLM*,  $| \cdot |$  is the number of blocks used for the key in *WorldLM*. In contrast,  $\nu$  is the number of layers we select for each residual across all clients. Finally,  $S_C$  are the parameters of the learning rate scheduler synchronized across **sequential** steps.

Model (size)	#Rounds	$\eta_s$	$\mu_s$	$  \cdot  $	$\nu$	$S_C( \cdot, \eta_m, x, T)$
English (75M)	12	0.2	0.9	1	1	$(10^{-4}, 8 \times 10^{-4}, 3 \times 10^3)$
English (125M)	21	0.2	0.9	3	1	$(10^{-4}, 6 \times 10^{-4}, 5 \times 10^3)$
Multi (25 M)	12	0.2	0.9	1	1	$(10^{-4}, 8 \times 10^{-4}, 5 \times 10^3)$

the **Pile Common Crawl**, **Wikipedia**, **PubMed Central**, and **PubMed Abstracts** datasets, then the node itself will hold data from them, proportionate to their size. For this dataset, we use the common *gpt-neox-20b* English tokenizer also adopted by Sani et al. [59]

To simulate geographically distributed systems, we use a subset of Multilingual Colossal Common Crawl (*mC4*) [80], covering high and low-resource languages [46]. We then build sub-federations based on language families similarly to *The Pile*. Given the larger vocabulary size [80] and consequent model size, we use a single federated structure partitioned with the high-resource French (**FR**) and Italian (**IT**) on one side and the lower-resource Bulgarian (**BG**) and Ukrainian (**UK**) on the other. For IID experiments, we use the standard Cleaned Colossal Common Crawl (*C4*) English dataset, partitioned into equal-sized shards with the same tokenizer as *The Pile*.

#### 4.1 Tasks

For all experiments, we use decoder-only transformers [9] for the language modeling task. Given that we are concerned with partially personalized FL, we compare the personalized **local** perplexity of *WorldLM* against three relevant baselines representing alternative scenarios. First, we compare against our closest alternative, standard FL with momentum [28, 13, 59], which has no hierarchical structure and would be difficult to integrate across legally and organizationally heterogeneous participants given the aforementioned governance issues. Second, we compare against independently trained fully personalized local models which do not share information, thus being heavily constrained by the local dataset size. This may result in heavy memorization due to overfitting to the limited amount of data of one organization. Third, we compare against centralized training of a global model on all the node’s data pooled together, irrespective of privacy concerns. The centralized baseline approximates the upper bound performance for a global model.

**Language Modelling:** We focus on an underrepresented segment: groups having access to a meaningful but not sufficient number of GPUs. For example, organizations holding 8 NVIDIA A40s (as we use in this work). In such scenarios, while billion-scale LMs may be out of reach due to sheer VRAM and bandwidth requirements, medium models may be practically useful (e.g., by providing highly relevant embeddings) without possessing the externalities of pre-trained models. Thus, given the hardware, we use three scales of models (75M, 125M, and 250M). Our federated training uses the parameters shown in Table 1 while the local parameters are available in Table 4. We compare models that have executed for a given number of **sequential** steps, the step-wise execution

we chose for *WorldLM* (Algorithm 1) implies that each level of a hierarchy (Fig. 1) trains in parallel; however, the levels execute sequentially relative to each other in **three** stages.

**Privacy and Security:** To validate the effectiveness of *WorldLM* for enhancing privacy and security, we simulate differentially private training, in which the leaves of a hierarchy contain potentially sensitive information and thus use *DPFed-vg* [72, 2] instead of standard averaging. This requires gradient clipping and the injection of Gaussian noise. To this end, we assumed that the **Pile-CC** and **WK** leaf clients of *The Pile* require DP and inject noise with  $\sigma = 0.5$  while clipping their gradients to the median  $l_1$  norm of the previous round (for the first round we use a bound of 1.0 as done for centralized ML [61]). Given the hierarchical training of *WorldLM* and the personalization involved, we postulate that it can more effectively account for the DP noise.

## 5 Evaluation

Our results for the language modeling task (Table 2) show that *WorldLM* offers the desired compromise between global performance and local personalization. *WorldLM* is capable of outperforming standard FL in terms of **local** personalized performance for datasets that exhibit statistical heterogeneity, while obtaining similar performance on the IID *C4* dataset. Furthermore, it approaches a fully-centralized baseline for the 75M model trained on *The Pile* and the 250M model trained on *mC4*. As can be seen in Fig. 3, the **partially-personalized aggregation** of *WorldLM* allows it to approach the performance of a centralized model despite data never leaving each organization’s premises. This holds the promise of international collaboration towards the federated training of LLMs. Since *WorldLM* executes in three stages (Algorithm 1) for a 3-level hierarchy, Fig. 3 exhibits temporary **perplexity spikes** in the convergence curve (e.g, the triangle formed by rounds 18–21 in Fig. 3). We chose to show all three stages since they correspond to different **sequential** steps. Thus, the root executes by itself while all nodes on a level execute together. For comparisons not dependent on the stage, consult Table 2.

Similar results can be observed on our heterogeneous partition of *The Pile* in Fig. 4. However, the smaller heterogeneity between English texts causes a smaller gap between *WorldLM* and standard FL. We use the 75M model and *The Pile* to evaluate the resilience of *WorldLM* to differential privacy and changes in the data hierarchy (Fig. 2) due to being compute-limited.

We evaluate the robustness of *WorldLM* to differential privacy and using an **alternative** arrangement of *The Pile* which does not contain an inherent cluster relationship. The main limitation of *WorldLM* is an imperfect ability to reconcile hierarchies with a high degree of intra-federation heterogeneity. As can be seen Table 3 and Fig. 5 swapping the data of **WK** with **PB** (Fig. 2) results in worse performance compared to standard FL due to the  $\mathcal{K}$  layers of the root being unable to agree during attention-based aggregation. Crucially, as can be observed from Fig. 5, the personalized layers of the other nodes, together with the residual mechanism of *WorldLM* allow them to maintain performance despite this decrease for the root. Consequently, for a majority of the participating organizations *WorldLM* serves as a superior alternative to FL from a personalization perspective.

Table 2: Language modeling personalized performance (over **local** client test sets) of *WorldLM* in terms of perplexity (the lower, the better). We compare against standard FL, fully local, and centralized models. The latter is trained on the union of all local training sets. *WorldLM* outperforms standard FL across all Non-IID dataset partitions, reaching a perplexity almost twice lower for *mC4*. While fully local models may seem to perform well, they are unlikely to generalize out of distribution and are prone towards divergence due to small dataset sizes, as seen in Fig. 3.

Dataset	Model	Collaborative		Non-Collaborative	
		<i>World M</i>	FL	Local	Centralized
<b>Pile</b>	<b>75M</b>	<b>73.82 ± 44.18</b>	107.31 ± 52.50	<b>4 .66 ± 25.28</b>	85.81 ± 24.42
<b>Pile</b>	<b>125M</b>	<b>48.34 ± 32.41</b>	53.92 ± 24.24	<b>24.83 ± 12.47</b>	29.61 ± 13.17
<b>MC4</b>	<b>250M</b>	<b>8 .47 ± 68.53</b>	153.27 ± 95.47	<b>45.47 ± 31.13</b>	72.21 ± 49.78
<b>C4</b>	<b>75M</b>	167.31 ± 2.92	<b>145.32 ± 3.53</b>	N/A	67.01 ± 1.67



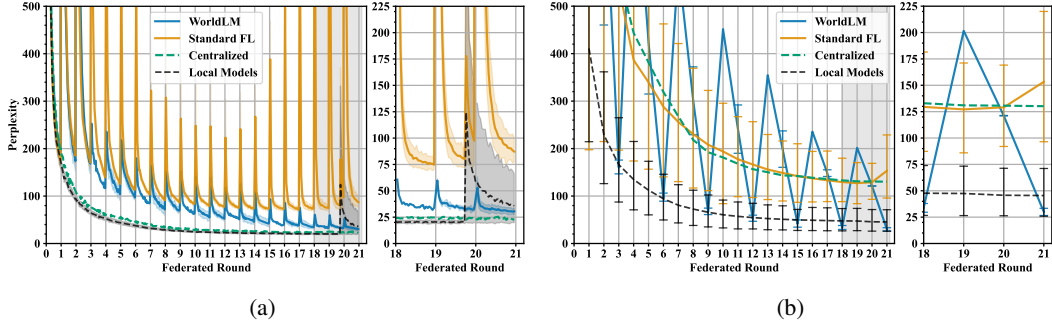


Figure 3: *WorldLM* training (a) and validation (b) **local** performance of the 250M multilingual model trained on a three-level heterogeneous partitioning of *mC4* constructed analogously to Fig. 2 and composed of the high-resource *Italian* and *French* languages on one side with the lower-resource *Ukrainian* and *Bulgarian* on the other. While standard FL stops improving after round 15, *WorldLM* reaches a performance close to the local and centralized models. The spike in local model perplexity at the end is due to eventual overtraining on the small *Bulgarian* and *Ukrainian* datasets.

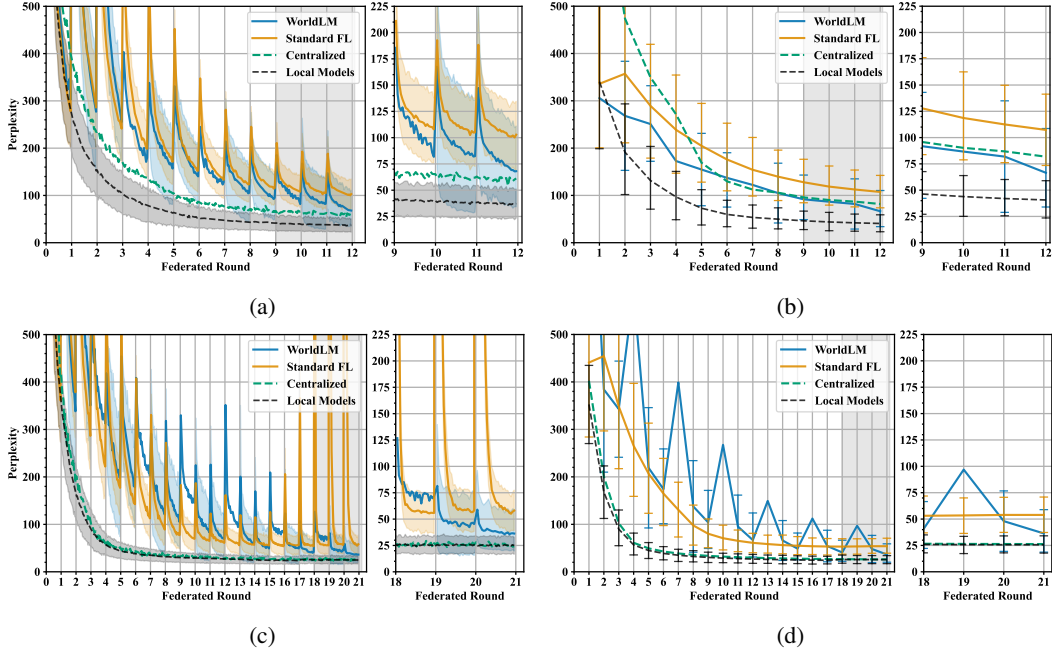


Figure 4: *WorldLM* training and validation performance of the 75M (a, b) and 125M (c, d) English models on a three-level heterogeneous partitioning of *The Pile* (Fig. 2). While the hierarchical approach makes steady progress due to its attention-based aggregation and partial personalization, standard FL struggles to converge due to data heterogeneity. Crucially, the performance of *WorldLM* approaches that of the centralized model and partially overlaps with overfitted local models.



Table 3: Results evaluating privacy and robustness. *WorldLM* is highly resilient to DP with  $\sigma = 0.5$  being applied over two of its leaf participants due to its aggregation procedure and because they start from a better initialization due to parent training. By contrast, the high amount of noise causes the entire global model of standard FL to diverge, without any personalized portions to maintain the performance of the non-DP members. Regarding robustness, *WorldLM* suffers a decrease in performance once the cluster relationship in Fig. 2 is broken in **Pile** ( ) but remains competitive.

Method	Pile	DP <sub>CC WK</sub>	DP <sub>PBC PBA</sub>	Pile ( )
<i>WorldLM</i>	$73.82 \pm 44.18$	$11.78 \pm 88.48$	$13.68 \pm 9.53$	$140.05 \pm 100.52$
<b>FL</b>	$107.31 \pm 52.50$	$724.56 \pm 251.89$	$724.24 \pm 250.98$	$17.31 \pm 52.5$

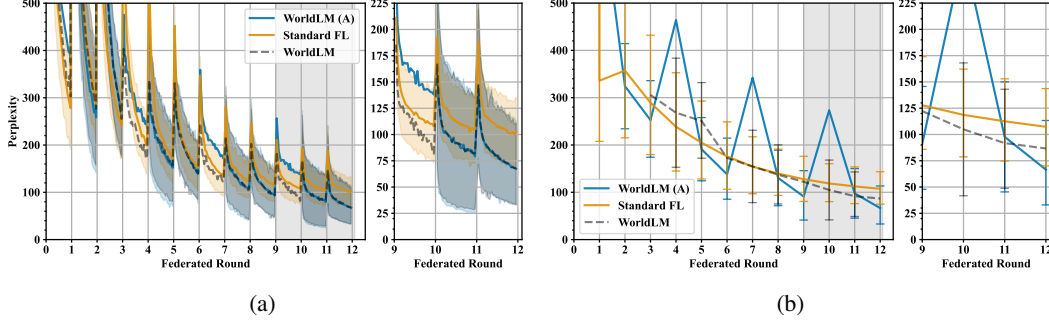


Figure 5: The impact of swapping **WK** with **PB** for *The Pile* dataset (see Fig. 2) for our 75M model. The swap results in the root node having worse performance (rounds 6–7 and 9–10) due to being unable to reconcile the conflicting update directions from its sub-federations. Despite this fact, the personalized  $\mathcal{K}$  layers of the other nodes adjust the backbone  $\mathcal{B}$  to their local distribution. The **cross-federation information sharing** also permits the parameters of similar nodes (e.g. **PB** and **PBC**) to jointly optimize their keys, preserving overall **local** test-set performance.

Table 3 shows that *WorldLM* is generally more robust than standard FL to the gradient clipping and noise that DP injects into the models of two leaf nodes. Standard FL diverges immediately due to its inability to suppress the impact of DP on the global model. The personalized keys of *WorldLM*, on the other hand, can ignore the impact of the noise entirely, as seen in Fig. 6. Furthermore, the additional per-level momentum mechanism of *WorldLM* allows it to stabilize the backbone training. This indicates that additional means of accounting for noise may be highly beneficial for standard FL approaches as well. For example, first pre-training on non-DP clients.

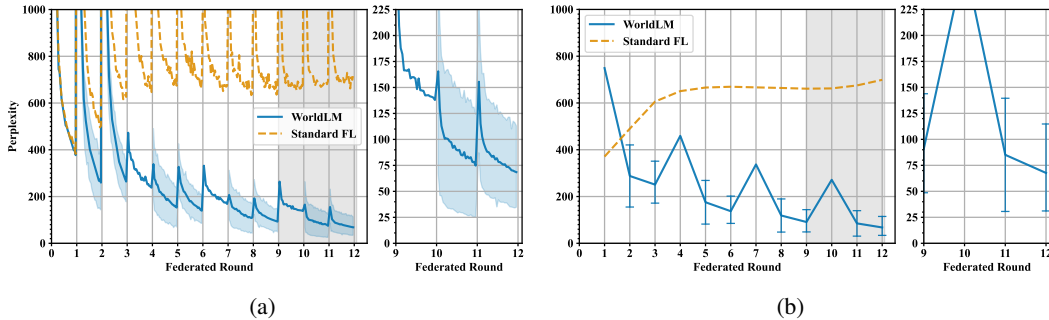


Figure 6: The impact of differential privacy on *WorldLM* performance, with the 75M model on *The Pile*, versus standard FL when using Gaussian noise with  $\sigma = 0.5$  and clipping client pseudo-gradients to the median pre-clip norm of the previous round. *WorldLM* is able to stabilize the training and validation performance (a,b) when applying DP over the leaf **CC** and **WK** clients, unlike FL which diverges. While the attentional aggregation and parent-regularization maintain *WorldLM* performance, standard FL allows the noise of even two clients to diverge the entirety of the aggregation procedure.

## 6 Conclusion

*WorldLM* supports the extension of federated learning (FL) to the challenging setting of worldwide optimization of language models (LMs). Our results indicate that systems based on **federations-of-federations** can compete with standard FL and centralized optimization for the medium-sized LMs affordable to small organizations and groups, given their hardware. Our results show that *WorldLM* can outperform standard FL under realistic federated topologies and data distributions constructed using naturally heterogeneous datasets. Furthermore, they also indicate our method to be robust under the constraints of differential privacy, unlike standard FL. Thus, *WorldLM* is an effective approach for addressing the nascent sub-field of worldwide LM pre-training. We open several new research opportunities such as: (a) bringing the benefits of *WorldLM* to the larger models that wealthy organizations can afford, (b) tackling broader forms of statistical heterogeneity, and (c) applying it to parameter-efficient fine-tuning. We hope this will help democratize LM training across national boundaries and address the societal concerns regarding its governance.

## Acknowledgments and Disclosure of Funding

This work was conducted with the support of the Ministry of Education of Romania through the Credit and Scholarship Agency.

## References

- [1] M. S. H. Abad, E. Ozfatura, D. Gündüz, and . Erçetin. Hierarchical federated learning ACROSS heterogeneous cellular networks. In *2020 IEEE International Conference on Acoustics, Speech and Signal Processing, ICASSP 2020, Barcelona, Spain, May 4-8, 2020*, pages 8866–8870. IEEE, 2020. doi: 10.1109/ICASSP40776.2020.9054634. URL <https://doi.org/10.1109/ICASSP40776.2020.9054634>.
- [2] G. Andrew, O. Thakkar, B. McMahan, and S. Ramaswamy. Differentially private learning with adaptive clipping. In M. Ranzato, A. Beygelzimer, Y. N. Dauphin, P. Liang, and J. W. Vaughan, editors, *Advances in Neural Information Processing Systems 34: Annual Conference on Neural Information Processing Systems 2021, NeurIPS 2021, December 6-14, 2021, virtual*, pages 17455–17466, 2021. URL <https://proceedings.neurips.cc/paper/2021/hash/91cff01af640a24e7f9f7a5ab407889f-bstract.html>.
- [3] M. G. Arivazhagan, V. Aggarwal, A. K. Singh, and S. Choudhary. Federated learning with personalization layers. *CoRR*, abs/1912.00818, 2019. URL <http://arxiv.org/abs/1912.00818>.
- [4] A. Baez and H. Saggion. LSLlama: Fine-tuned LLaMA for lexical simplification. In S. Štajner, H. Saggio, M. Shardlow, and F. Alva-Manchego, editors, *Proceedings of the Second Workshop on Text Simplification, Accessibility and Readability*, pages 102–108, Varna, Bulgaria, Sept. 2023. INCOMA Ltd., Shoumen, Bulgaria. URL <https://aclanthology.org/2023.tsar-1.10>.
- [5] R. Bommasani, D. A. Hudson, E. Adeli, R. B. Altman, S. Arora, and et al. On the opportunities and risks of foundation models. *CoRR*, abs/2108.07258, 2021. URL <https://arxiv.org/abs/2108.07258>.
- [6] K. A. Bonawitz, V. Ivanov, B. Kreuter, A. Marcedone, H. B. McMahan, S. Patel, D. Ramage, A. Segal, and K. Seth. Practical secure aggregation for federated learning on user-held data. *CoRR*, abs/1611.04482, 2016. URL <http://arxiv.org/abs/1611.04482>.
- [7] K. A. Bonawitz, H. Eichner, W. Grieskamp, D. Huba, A. Ingerman, V. Ivanov, C. Kidon, J. Konečný, S. Mazzocchi, B. McMahan, T. V. Overveldt, D. Petrou, D. Ramage, and J. Roselander. Towards federated learning at scale: System design. In A. Talwalkar, V. Smith, and M. Zaharia, editors, *Proceedings of Machine Learning and Systems 2019, MLSys 2019, Stanford, CA, USA, March 31 - April 2, 2019*. mlsys.org, 2019. URL <https://proceedings.mlsys.org/book/271.pdf>.

- [8] C. Briggs, Z. Fan, and P. Andras. Federated learning with hierarchical clustering of local updates to improve training on non-iid data. In *2020 International Joint Conference on Neural Networks, IJCNN 2020, Glasgow, United Kingdom, July 19-24, 2020*, pages 1–9. IEEE, 2020. doi: 10.1109/IJCNN48605.2020.9207469. URL <https://doi.org/10.1109/IJCNN48605.2020.9207469>.
- [9] T. B. Brown, B. Mann, N. Ryder, M. Subbiah, J. Kaplan, P. Dhariwal, A. Neelakantan, P. Shyam, G. Sastry, A. Askell, S. Agarwal, A. Herbert-Voss, G. Krueger, T. Henighan, R. Child, A. Ramesh, D. M. Ziegler, J. Wu, C. Winter, C. Hesse, M. Chen, E. Sigler, M. Litwin, S. Gray, B. Chess, J. Clark, C. Berner, S. McCandlish, A. Radford, I. Sutskever, and D. Amodei. Language models are few-shot learners, 2020.
- [10] Z. Charles, Z. Garrett, Z. Huo, S. Shmulyian, and V. Smith. On large-cohort training for federated learning. In M. Ranzato, A. Beygelzimer, Y. N. Dauphin, P. Liang, and J. W. Vaughan, editors, *Advances in Neural Information Processing Systems 34: Annual Conference on Neural Information Processing Systems 2021, NeurIPS 2021, December 6-14, 2021, virtual*, pages 20461–20475, 2021. URL <https://proceedings.neurips.cc/paper/2021/hash/ab9ebd57177b5106ad7879f0896685d4-bstract.html>.
- [11] G. Cheng, K. N. Chadha, and J. C. Duchi. Fine-tuning is fine in federated learning. *CoRR*, abs/2108.07313, 2021. URL <https://arxiv.org/abs/2108.07313>.
- [12] Council of European Union, Apr 2021. Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL - LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206>. Document 52021PC0206.
- [13] A. Douillard, Q. Feng, A. A. Rusu, R. Chhaparia, Y. Donchev, A. Kuncoro, M. Ranzato, A. Szlam, and J. Shen. Diloco: Distributed low-communication training of language models. *CoRR*, abs/2311.08105, 2023. doi: 10.48550/ARXIV.2311.08105. URL <https://doi.org/10.48550/arXiv.2311.08105>.
- [14] C. Dwork, F. McSherry, K. Nissim, and A. D. Smith. Calibrating noise to sensitivity in private data analysis. *J. Priv. Confidentiality*, 7(3):17–51, 2016. doi: 10.29012/JPC.V7I3.405. URL <https://doi.org/10.29012/jpc.v7i3.405>.
- [15] European Parliament and Council of the European Union. Regulation (EU) 2016/679 of the European Parliament and of the Council, 2016. URL <https://data.europa.eu/eli/reg/2016/679/oj>.
- [16] F. Faisal, Y. Wang, and A. Anastasopoulos. Dataset geography: Mapping language data to language users. In S. Muresan, P. Nakov, and A. Villavicencio, editors, *Proceedings of the 60th Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers), CL 2022, Dublin, Ireland, May 22-27, 2022*, pages 3381–3411. Association for Computational Linguistics, 2022. doi: 10.18653/V1/2022.ACL-LONG.239. URL <https://doi.org/10.18653/v1/2022.acl-long.239>.
- [17] A. Fallah, A. Mokhtari, and A. E. Ozdaglar. Personalized federated learning with theoretical guarantees: A model-agnostic meta-learning approach. In H. Larochelle, M. Ranzato, R. Hadsell, M. Balcan, and H. Lin, editors, *Advances in Neural Information Processing Systems 33: Annual Conference on Neural Information Processing Systems 2020, NeurIPS 2020, December 6-12, 2020, virtual*, 2020. URL <https://proceedings.neurips.cc/paper/2020/hash/24389bfe4fe2eba8bf9aa9203a44cdad-bstract.html>.
- [18] L. Gao, S. Biderman, S. Black, L. Golding, T. Hoppe, C. Foster, J. Phang, H. He, A. Thite, N. Nabeshima, S. Presser, and C. Leahy. The pile: An 800gb dataset of diverse text for language modeling. *CoRR*, abs/2101.00027, 2021. URL <https://arxiv.org/abs/2101.00027>.
- [19] A. P. Gema, L. Daines, P. Minervini, and B. Alex. Parameter-efficient fine-tuning of llama for the clinical domain. *CoRR*, abs/2307.03042, 2023. doi: 10.48550/ARXIV.2307.03042. URL <https://doi.org/10.48550/arXiv.2307.03042>.

- [20] A. Ghosh, J. Chung, D. Yin, and K. Ramchandran. An efficient framework for clustered federated learning. *IEEE Trans. Inf. Theory*, 68(12):8076–8091, 2022. doi: 10.1109/TIT.2022.3192506. URL <https://doi.org/10.1109/TIT.2022.3192506>.
- [21] J. González-García, F. Estupiñán-Romero, C. Tellería-Orriols, J. González-Galindo, L. Palmieri, A. Faragalli, I. Pristās, J. Vuković, J. Misinš, I. Zile, E. Bernal-Delgado, B. Unim, F. Carle, R. Gesuita, D. Ivanković, M. Brkić, J. Dimnjaković, J. Lyons, R. Lyons, Z. Ors, M. Zaletel, P. Nogueira, L. V. Lapão, H. Haaheim, P. Bogaert, L. Abboud, H. van Oyen, and o. b. o. t. I. J. A. consortium. Coping with interoperability in the development of a federated research infrastructure: achievements, challenges and recommendations from the JA-InfAct. *Archives of Public Health*, 79(1):221, Dec 2021. ISSN 2049-3258. doi: 10.1186/s13690-021-00731-z. URL <https://doi.org/10.1186/s13690-021-00731-z>.
- [22] M. M. Grynbaum and R. Mac. The times sues openai and microsoft over a.i. use of copyrighted work, Dec 2023. URL <https://www.nytimes.com/2023/12/27/business/media/new-york-times-open-ai-microsoft-lawsuit.html>.
- [23] K. He, X. Zhang, S. Ren, and J. Sun. Deep residual learning for image recognition. In *2016 IEEE Conference on Computer Vision and Pattern Recognition, CVPR 2016, Las Vegas, NV, US, June 27-30, 2016*, pages 770–778. IEEE Computer Society, 2016. doi: 10.1109/CVPR.2016.90. URL <https://doi.org/10.1109/CVPR.2016.90>.
- [24] J. Hoffmann, S. Borgeaud, A. Mensch, E. Buchatskaya, T. Cai, E. Rutherford, D. de Las Casas, L. A. Hendricks, J. Welbl, A. Clark, T. Hennigan, E. Noland, K. Millican, G. van den Driessche, B. Damoc, A. Guy, S. Osindero, K. Simonyan, E. Elsen, J. W. Rae, O. Vinyals, and L. Sifre. Training compute-optimal large language models. *CoRR*, abs/2203.15556, 2022. doi: 10.48550/ARXIV.2203.15556. URL <https://doi.org/10.48550/arXiv.2203.15556>.
- [25] E. J. Hu, Y. Shen, P. Wallis, Z. Allen-Zhu, Y. Li, S. Wang, L. Wang, and W. Chen. Lora: Low-rank adaptation of large language models, 2021.
- [26] Y. Huang, L. Chu, Z. Zhou, L. Wang, J. Liu, J. Pei, and Y. Zhang. Personalized cross-silo federated learning on non-iid data. In *Thirty-Fifth AAAI Conference on Artificial Intelligence, AAAI 2021, Thirty-Third Conference on Innovative Applications of Artificial Intelligence, IAAI 2021, The Eleventh Symposium on Educational Advances in Artificial Intelligence, EAAI 2021, Virtual Event, February 2-9, 2021*, pages 7865–7873. AAAI Press, 2021. URL <https://ojs.aaai.org/index.php/AAAI/article/view/16960>.
- [27] D. Huba, J. Nguyen, K. Malik, R. Zhu, M. Rabbat, A. Yousefpour, C. Wu, H. Zhan, P. Ustinov, H. Srinivas, K. Wang, A. Shoumikhin, J. Min, and M. Malek. PAPAYA: practical, private, and scalable federated learning. In D. Marculescu, Y. Chi, and C. Wu, editors, *Proceedings of Machine Learning and Systems 2022, MLSys 2022, Santa Clara, CA, USA, August 29 - September 1, 2022*. mlsys.org, 2022. URL <https://proceedings.mlsys.org/paper/2022/hash/f340f1b1f65b6df5b5e3f94d95b11daf-bstract.html>.
- [28] Z. Huo, Q. Yang, B. Gu, L. Carin, and H. Huang. Faster on-device training using new federated momentum algorithm. *CoRR*, abs/2002.02090, 2020. URL <https://arxiv.org/abs/2002.02090>.
- [29] S. Ji, S. Pan, G. Long, X. Li, J. Jiang, and Z. Huang. Learning private neural language modeling with attentive aggregation. In *International Joint Conference on Neural Networks, IJCNN 2019 Budapest, Hungary, July 14-19, 2019*, pages 1–8. IEEE, 2019. doi: 10.1109/IJCNN.2019.8852464. URL <https://doi.org/10.1109/IJCNN.2019.8852464>.
- [30] M. Joblin, B. Eckl, T. Bock, A. Schmid, J. Siegmund, and S. Apel. Hierarchical and hybrid organizational structures in open-source software projects: A longitudinal study. *CM Trans. Softw. Eng. Methodol.*, 32(4):86:1–86:29, 2023. doi: 10.1145/3569949. URL <https://doi.org/10.1145/3569949>.
- [31] M. Joshi, A. Pal, and M. Sankarasubbu. Federated learning for healthcare domain - pipeline, applications and challenges. *CM Trans. Comput. Heal.*, 3(4):40:1–40:36, 2022. doi: 10.1145/3533708. URL <https://doi.org/10.1145/3533708>.

- [32] S. Kadhe, N. Rajaraman, O. O. Koyluoglu, and K. Ramchandran. Fastsecagg: Scalable secure aggregation for privacy-preserving federated learning. *CoRR*, abs/2009.11248, 2020. URL <https://arxiv.org/abs/2009.11248>.
- [33] P. Kairouz, H. B. McMahan, B. Avent, A. Bellet, M. Bennis, and et al. Advances and open problems in federated learning. *Found. Trends Mach. Learn.*, 14(1-2):1–210, 2021. doi: 10.1561/22000000083. URL <https://doi.org/10.1561/22000000083>.
- [34] J. Kaplan, S. McCandlish, T. Henighan, T. B. Brown, B. Chess, R. Child, S. Gray, A. Radford, J. Wu, and D. Amodei. Scaling laws for neural language models. *CoRR*, abs/2001.08361, 2020. URL <https://arxiv.org/abs/2001.08361>.
- [35] N. S. Keskar, D. Mudigere, J. Nocedal, M. Smelyanskiy, and P. T. P. Tang. On large-batch training for deep learning: Generalization gap and sharp minima. In *5th International Conference on Learning Representations, ICLR 2017, Toulon, France, April 24-26, 2017, Conference Track Proceedings*. OpenReview.net, 2017. URL <https://openreview.net/forum?id=H1oyRlYgg>.
- [36] B. Klievink, H. V. D. Voort, and W. Veeneman. Creating value through data collaboratives. *Inf. Policy*, 23(4):379–397, 2018. doi: 10.3233/IP-180070. URL <https://doi.org/10.3233/IP-180070>.
- [37] R. Lee, M. Kim, D. Li, X. Qiu, T. M. Hospedales, F. Huszar, and N. D. Lane. Fedl2p: Federated learning to personalize. In A. Oh, T. Naumann, A. Globerson, K. Saenko, M. Hardt, and S. Levine, editors, *Advances in Neural Information Processing Systems 36: Annual Conference on Neural Information Processing Systems 2023, NeurIPS 2023, New Orleans, LA, US, December 10 - 16, 2023*, 2023. URL [http://papers.nips.cc/paper\\_files/paper/2023/hash/2fb57276bfba1b832d7bfcb36bb41c-bstract-Conference.html](http://papers.nips.cc/paper_files/paper/2023/hash/2fb57276bfba1b832d7bfcb36bb41c-bstract-Conference.html).
- [38] Q. Li, Y. Diao, Q. Chen, and B. He. Federated learning on non-iid data silos: An experimental study. In *38th IEEE International Conference on Data Engineering, ICDE 2022, Kuala Lumpur, Malaysia, May 9-12, 2022*, pages 965–978. IEEE, 2022. doi: 10.1109/ICDE53745.2022.00077. URL <https://doi.org/10.1109/ICDE53745.2022.00077>.
- [39] Z. Li, S. Si, J. Wang, and J. Xiao. Federated split BERT for heterogeneous text classification. In *International Joint Conference on Neural Networks, IJCNN 2022, Padua, Italy, July 18-23, 2022*, pages 1–8. IEEE, 2022. doi: 10.1109/IJCNN55064.2022.9892845. URL <https://doi.org/10.1109/IJCNN55064.2022.9892845>.
- [40] T. Lin, S. U. Stich, K. K. Patel, and M. Jaggi. Don’t use large mini-batches, use local SGD. In *8th International Conference on Learning Representations, ICLR 2020, Addis Ababa, Ethiopia, April 26-30, 2020*. OpenReview.net, 2020. URL <https://openreview.net/forum?id=B1ey01BFPr>.
- [41] L. Liu, J. Zhang, S. Song, and K. B. Letaief. Client-edge-cloud hierarchical federated learning. In *2020 IEEE International Conference on Communications, ICC 2020, Dublin, Ireland, June 7-11, 2020*, pages 1–6. IEEE, 2020. doi: 10.1109/ICC40277.2020.9148862. URL <https://doi.org/10.1109/ICC40277.2020.9148862>.
- [42] Y. Liu, J. Cao, C. Liu, K. Ding, and L. Jin. Datasets for large language models: A comprehensive survey. *CoRR*, abs/2402.18041, 2024. doi: 10.48550/ARXIV.2402.18041. URL <https://doi.org/10.48550/arXiv.2402.18041>.
- [43] S. Luo, X. Chen, Q. Wu, Z. Zhou, and S. Yu. HFEL: joint edge association and resource allocation for cost-efficient hierarchical federated edge learning. *IEEE Trans. Wirel. Commun.*, 19(10):6535–6548, 2020. doi: 10.1109/TWC.2020.3003744. URL <https://doi.org/10.1109/TWC.2020.3003744>.
- [44] L. Lyu, J. Yu, K. Nandakumar, Y. Li, X. Ma, J. Jin, H. Yu, and K. S. Ng. Towards fair and privacy-preserving federated deep models. *IEEE Trans. Parallel Distributed Syst.*, 31(11):2524–2541, 2020. doi: 10.1109/TPDS.2020.2996273. URL <https://doi.org/10.1109/TPDS.2020.2996273>.

- [45] S. Ma, H. Wang, L. Ma, L. Wang, W. Wang, S. Huang, L. Dong, R. Wang, J. Xue, and F. Wei. The era of 1-bit llms: All large language models are in 1.58 bits. *CoRR*, abs/2402.17764, 2024. doi: 10.48550/ARXIV.2402.17764. URL <https://doi.org/10.48550/arXiv.2402.17764>.
- [46] A. Magueresse, V. Carles, and E. Heetderks. Low-resource languages: A review of past work and future challenges. *CoRR*, abs/2006.07264, 2020. URL <https://arxiv.org/abs/2006.07264>.
- [47] Y. Mansour, M. Mohri, J. Ro, and A. T. Suresh. Three approaches for personalization with applications to federated learning. *CoRR*, abs/2002.10619, 2020. URL <https://arxiv.org/abs/2002.10619>.
- [48] B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y Arcas. Communication-efficient learning of deep networks from decentralized data. In A. Singh and X. J. Zhu, editors, *Proceedings of the 20th International Conference on Artificial Intelligence and Statistics, ISTATS 2017, 20-22 April 2017, Fort Lauderdale, FL, US*, volume 54 of *Proceedings of Machine Learning Research*, pages 1273–1282. PMLR, 2017. URL <http://proceedings.mlr.press/v54/mcmahan17a.html>.
- [49] H. B. McMahan, D. Ramage, K. Talwar, and L. Zhang. Learning differentially private recurrent language models. In *6th International Conference on Learning Representations, ICLR 2018, Vancouver, BC, Canada, April 30 - May 3, 2018, Conference Track Proceedings*. OpenReview.net, 2018. URL <https://openreview.net/forum?id=BJ0hF1Z0b>.
- [50] Meta. Introducing Meta Llama 3: The most capable openly available LLM to date, Apr 2024. URL <https://ai.meta.com/blog/meta-llama-3/>.
- [51] N. Mhaisen, A. A. Abdellatif, A. Mohamed, A. Erbad, and M. Guizani. Optimal user-edge assignment in hierarchical federated learning based on statistical properties and network topology constraints. *IEEE Trans. Netw. Sci. Eng.*, 9(1):55–66, 2022. doi: 10.1109/TNSE.2021.3053588. URL <https://doi.org/10.1109/TNSE.2021.3053588>.
- [52] A. Nichol, J. Achiam, and J. Schulman. On first-order meta-learning algorithms. *CoRR*, abs/1803.02999, 2018. URL <http://arxiv.org/abs/1803.02999>.
- [53] OpenAI, Dec 2023. URL <https://openai.com/blog/axel-springer-partnership>.
- [54] S. Patel and S. Palazzolo. OpenAI offers publishers as little as \$1 million a year — the information, Jan 2024. URL <https://www.theinformation.com/articles/openai-offers-publishers-as-little-as-1-million-a-year>.
- [55] S. Pati, U. Baid, B. Edwards, M. J. Sheller, H. S. Wang, G. A. Reina, P. Foley, A. Gruzdev, D. Karkada, C. Davatzikos, C. Sako, S. Ghodasara, M. Bilello, S. Mohan, P. Vollmuth, G. Brugnara, C. J. Preetha, F. Sahm, K. H. Maier-Hein, M. Zenk, M. Bendszus, W. Wick, E. Calabrese, J. D. Rudie, J. E. Villanueva-Meyer, S. Cha, M. Ingahalikar, M. Jadhav, U. Pandey, J. Saini, J. Garrett, M. Larson, R. Jeraj, S. Currie, R. Frood, K. Fatania, R. Y. Huang, K. Chang, C. B. Quintero, J. Capellades, J. Puig, J. Trenkler, J. Pichler, G. Necker, A. Haunschmidt, S. Meckel, G. Shukla, S. Liem, G. S. Alexander, and et al. Federated learning enables big data for rare cancer boundary detection. *CoRR*, abs/2204.10836, 2022. doi: 10.48550/arXiv.2204.10836. URL <https://doi.org/10.48550/arXiv.2204.10836>.
- [56] S. Rajbhandari, J. Rasley, O. Ruwase, and Y. He. Zero: memory optimizations toward training trillion parameter models. In C. Cuicchi, I. Qualters, and W. T. Kramer, editors, *Proceedings of the International Conference for High Performance Computing, Networking, Storage and Analysis, SC 2020, Virtual Event / Atlanta, Georgia, US, November 9-19, 2020*, page 20. IEEE/ACM, 2020. doi: 10.1109/SC41405.2020.00024. URL <https://doi.org/10.1109/SC41405.2020.00024>.
- [57] S. Ranathunga, E. A. Lee, M. P. Skenduli, R. Shekhar, M. Alam, and R. Kaur. Neural machine translation for low-resource languages: A survey. *CM Comput. Surv.*, 55(11):229:1–229:37, 2023. doi: 10.1145/3567592. URL <https://doi.org/10.1145/3567592>.

- [58] S. J. Reddi, Z. Charles, M. Zaheer, Z. Garrett, K. Rush, J. Konečný, S. Kumar, and H. B. McMahan. Adaptive federated optimization. In *9th International Conference on Learning Representations, ICLR 2021, Virtual Event, Austria, May 3-7, 2021*. OpenReview.net, 2021. URL <https://openreview.net/forum?id=LkFG3lB13U5>.
- [59] L. Sani, A. Iacob, Z. Cao, B. Marino, Y. Gao, T. Paulik, W. Zhao, W. F. Shen, P. Aleksandrov, X. Qiu, and N. D. Lane. The future of large language model pre-training is federated, 2024.
- [60] F. Sattler, K. Müller, and W. Samek. Clustered federated learning: Model-agnostic distributed multitask optimization under privacy constraints. *IEEE Trans. Neural Networks Learn. Syst.*, 32(8):3710–3722, 2021. doi: 10.1109/TNNLS.2020.3015958. URL <https://doi.org/10.1109/TNNLS.2020.3015958>.
- [61] T. L. Scao, A. Fan, C. Akiki, E. Pavlick, S. Ilıc, D. Hesslow, R. Castagné, A. S. Luccioni, F. Yvon, M. Gallé, J. Tow, A. M. Rush, S. Biderman, A. Webson, P. S. Ammanamanchi, T. Wang, B. Sagot, N. Muennighoff, A. V. del Moral, O. Ruwase, R. Bawden, S. Bekman, A. McMillan-Major, I. Beltagy, H. Nguyen, L. Saulnier, S. Tan, P. O. Suarez, V. Sanh, H. Laurençon, Y. Jernite, J. Launay, M. Mitchell, C. Raffel, A. Gokaslan, A. Simhi, A. Soroa, A. F. Aji, A. Alfassy, A. Rogers, A. K. Nitzav, C. Xu, C. Mou, C. Emezue, C. Klamm, C. Leong, D. van Strien, D. I. Adelani, and et al. BLOOM: A 176b-parameter open-access multilingual language model. *CoRR*, abs/2211.05100, 2022. doi: 10.48550/ARXIV.2211.05100. URL <https://doi.org/10.48550/arXiv.2211.05100>.
- [62] A. Sergeev and M. D. Balso. Horovod: fast and easy distributed deep learning in tensorflow. *CoRR*, abs/1802.05799, 2018. URL <http://arxiv.org/abs/1802.05799>.
- [63] M. J. Sheller, B. Edwards, G. A. Reina, J. Martin, S. Pati, A. Kotrotsou, M. Milchenko, W. Xu, D. Marcus, R. R. Colen, and S. Bakas. Federated learning in medicine: facilitating multi-institutional collaborations without sharing patient data. *Scientific Reports*, 10(1):12598, 2020. doi: 10.1038/s41598-020-69250-1. URL <https://doi.org/10.1038/s41598-020-69250-1>.
- [64] J. So, C. J. Nolet, C. Yang, S. Li, Q. Yu, R. E. Ali, B. Guler, and S. Avestimehr. Lightsecagg: a lightweight and versatile design for secure aggregation in federated learning. In D. Marculescu, Y. Chi, and C. Wu, editors, *Proceedings of Machine Learning and Systems 2022, MLSys 2022, Santa Clara, C , US , ugust 29 - September 1, 2022*. mlsys.org, 2022. URL <https://proceedings.mlsys.org/paper/2022/hash/d2ddea18f00665ce8623e36bd4e3c7c5-bstract.html>.
- [65] S. U. Stich. Local SGD converges fast and communicates little. In *7th International Conference on Learning Representations, ICLR 2019, New Orleans, L , US , May 6-9, 2019*. OpenReview.net, 2019. URL <https://openreview.net/forum?id=S1g2JnRcFX>.
- [66] H. Touvron, T. Lavril, G. Izacard, X. Martinet, M. Lachaux, T. Lacroix, B. Rozière, N. Goyal, E. Hambro, F. Azhar, A. Rodriguez, A. Joulin, E. Grave, and G. Lample. Llama: Open and efficient foundation language models. *CoRR*, abs/2302.13971, 2023. doi: 10.48550/arXiv.2302.13971. URL <https://doi.org/10.48550/arXiv.2302.13971>.
- [67] H. Touvron, L. Martin, K. Stone, P. Albert, A. Almahairi, Y. Babaei, N. Bashlykov, S. Batra, P. Bhargava, S. Bhosale, D. Bikel, L. Blecher, C. C. Ferrer, M. Chen, G. Cucurull, D. Esiobu, J. Fernandes, J. Fu, W. Fu, B. Fuller, C. Gao, V. Goswami, N. Goyal, A. Hartshorn, S. Hosseini, R. Hou, H. Inan, M. Kardas, V. Kerkez, M. Khabsa, I. Kloumann, A. Korenev, P. S. Koura, M.-A. Lachaux, T. Lavril, J. Lee, D. Liskovich, Y. Lu, Y. Mao, X. Martinet, T. Mihaylov, P. Mishra, I. Molybog, Y. Nie, A. Poulton, J. Reizenstein, R. Rungta, K. Saladi, A. Schelten, R. Silva, E. M. Smith, R. Subramanian, X. E. Tan, B. Tang, R. Taylor, A. Williams, J. X. Kuan, P. Xu, Z. Yan, I. Zarov, Y. Zhang, A. Fan, M. Kambadur, S. Narang, A. Rodriguez, R. Stojnic, S. Edunov, and T. Scialom. Llama 2: Open foundation and fine-tuned chat models, 2023.
- [68] J. van Angeren, C. F. Alves, and S. Jansen. Can we ask you to collaborate? analyzing app developer relationships in commercial platform ecosystems. *J. Syst. Softw.*, 113:430–445, 2016. doi: 10.1016/J.JSS.2015.11.025. URL <https://doi.org/10.1016/j.jss.2015.11.025>.



- [69] A. Vaswani, N. Shazeer, N. Parmar, J. Uszkoreit, L. Jones, A. N. Gomez, L. Kaiser, and I. Polosukhin. Attention is all you need. In I. Guyon, U. von Luxburg, S. Bengio, H. M. Wallach, R. Fergus, S. V. N. Vishwanathan, and R. Garnett, editors, *Advances in Neural Information Processing Systems 30: Annual Conference on Neural Information Processing Systems 2017, December 4-9, 2017, Long Beach, CA, USA*, pages 5998–6008, 2017. URL <https://proceedings.neurips.cc/paper/2017/hash/3f5ee243547dee91fbd053c1c4a845aa-bstract.html>.
- [70] P. Villalobos, J. Sevilla, L. Heim, T. Besiroglu, M. Hobbhahn, and A. Ho. Will we run out of data? an analysis of the limits of scaling datasets in machine learning. *CoRR*, abs/2211.04325, 2022. doi: 10.48550/ARXIV.2211.04325. URL <https://doi.org/10.48550/arXiv.2211.04325>.
- [71] Z. Wang, H. Xu, J. Liu, H. Huang, C. Qiao, and Y. Zhao. Resource-efficient federated learning with hierarchical aggregation in edge computing. In *40th IEEE Conference on Computer Communications, INFOCOM 2021, Vancouver, BC, Canada, May 10-13, 2021*, pages 1–10. IEEE, 2021. doi: 10.1109/INFOCOM42981.2021.9488756. URL <https://doi.org/10.1109/INFOCOM42981.2021.9488756>.
- [72] K. Wei, J. Li, M. Ding, C. Ma, H. H. Yang, F. Farokhi, S. Jin, T. Q. S. Quek, and H. V. Poor. Federated learning with differential privacy: Algorithms and performance analysis. *IEEE Trans. Inf. Forensics Secur.*, 15:3454–3469, 2020. doi: 10.1109/TIFS.2020.2988575. URL <https://doi.org/10.1109/TIFS.2020.2988575>.
- [73] White House. Consumer data privacy in a networked world: A framework for protecting privacy and promoting innovation in the global digital economy. *Journal of Privacy and Confidentiality*, 4(2), Mar. 2013. doi: 10.29012/jpc.v4i2.623. URL <http://journalprivacyconfidentiality.org/index.php/jpc/article/view/623>.
- [74] White House. Executive order on the safe, secure, and trustworthy development and use of artificial intelligence, Oct 2023.
- [75] H. Woisetschlager, A. Erben, B. Marino, S. Wang, N. D. Lane, R. Mayer, and H. Jacobsen. Federated learning priorities under the european union artificial intelligence act. *CoRR*, abs/2402.05968, 2024. doi: 10.48550/ARXIV.2402.05968. URL <https://doi.org/10.48550/arXiv.2402.05968>.
- [76] H. Woisetschlager, A. Erben, B. Marino, S. Wang, N. D. Lane, R. Mayer, and H. Jacobsen. Federated learning priorities under the european union artificial intelligence act. *CoRR*, abs/2402.05968, 2024. doi: 10.48550/ARXIV.2402.05968. URL <https://doi.org/10.48550/arXiv.2402.05968>.
- [77] Q. Wu, K. He, and X. Chen. Personalized federated learning for intelligent iot applications: A cloud-edge based framework. *IEEE Open J. Comput. Soc.*, 1:35–44, 2020. doi: 10.1109/OJCS.2020.2993259. URL <https://doi.org/10.1109/OJCS.2020.2993259>.
- [78] L. Xu, H. Xie, S. J. Qin, X. Tao, and F. L. Wang. Parameter-efficient fine-tuning methods for pretrained language models: A critical review and assessment. *CoRR*, abs/2312.12148, 2023. doi: 10.48550/ARXIV.2312.12148. URL <https://doi.org/10.48550/arXiv.2312.12148>.
- [79] X. Xu, J. Wu, M. Yang, T. Luo, X. Duan, W. Li, Y. Wu, and B. Wu. Information leakage by model weights on federated learning. In B. Zhang, R. A. Popa, M. Zaharia, G. Gu, and S. Ji, editors, *PPMLP’20: Proceedings of the 2020 Workshop on Privacy-Preserving Machine Learning in Practice, Virtual Event, USA, November, 2020*, pages 31–36. ACM, 2020. doi: 10.1145/3411501.3419423. URL <https://doi.org/10.1145/3411501.3419423>.
- [80] L. Xue, N. Constant, A. Roberts, M. Kale, R. Al-Rfou, A. Siddhant, A. Barua, and C. Raffel. mt5: A massively multilingual pre-trained text-to-text transformer. In K. Toutanova, A. Rumshisky, L. Zettlemoyer, D. Hakkani-Tür, I. Beltagy, S. Bethard, R. Cotterell, T. Chakraborty, and Y. Zhou, editors, *Proceedings of the 2021 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies, NAACL-HLT 2021, Online, June 6-11, 2021*, pages 483–498. Association for Computational Linguistics, 2021. doi: 10.18653/v1/2021.NAACL-MAIN.41. URL <https://doi.org/10.18653/v1/2021.naacl-main.41>.

- [81] M. Ye, X. Fang, B. Du, P. C. Yuen, and D. Tao. Heterogeneous federated learning: State-of-the-art and research challenges. *CM Comput. Surv.*, 56(3):79:1–79:44, 2024. doi: 10.1145/3625558. URL <https://doi.org/10.1145/3625558>.
- [82] T. Yu, E. Bagdasaryan, and V. Shmatikov. Salvaging federated learning by local adaptation. *CoRR*, abs/2002.04758, 2020. URL <https://arxiv.org/abs/2002.04758>.
- [83] V. Zantedeschi, A. Bellet, and M. Tommasi. Fully decentralized joint learning of personalized models and collaboration graphs. In S. Chiappa and R. Calandra, editors, *The 23rd International Conference on Artificial Intelligence and Statistics, IST TS 2020, 26-28 August 2020, Online [Palermo, Sicily, Italy]*, volume 108 of *Proceedings of Machine Learning Research*, pages 864–874. PMLR, 2020. URL <http://proceedings.mlr.press/v108/zantedeschi20a.html>.
- [84] Y. Zhao, A. Gu, R. Varma, L. Luo, C. Huang, M. Xu, L. Wright, H. Shojanazeri, M. Ott, S. Shleifer, A. Desmaison, C. Balioglu, P. Damania, B. Nguyen, G. Chauhan, Y. Hao, A. Mathews, and S. Li. Pytorch FSDP: experiences on scaling fully sharded data parallel. *Proc. VLDB Endow.*, 16(12):3848–3860, 2023. doi: 10.14778/3611540.3611569. URL <https://www.vldb.org/pvldb/vol16/p3848-huang.pdf>.
- [85] T. Zhou, Z. Lin, J. Zhang, and D. H. K. Tsang. Understanding model averaging in federated learning on heterogeneous data. *CoRR*, abs/2305.07845, 2023. doi: 10.48550/arXiv.2305.07845. URL <https://doi.org/10.48550/arXiv.2305.07845>.

## ppendix

Table 4: Architecture details and local training parameters for our 75M and 250M models. They represent the number of transformer blocks, hidden model dimension, number of attention heads, the linear layer expansion ratio and the parameters of Adam.

Model (size)	#Blocks	$d$	#Heads	Exp. Ratio	$(\beta_1, \beta_2)$	Vocab
English (75M)	3	896	16	4	(0.9, 0.95)	50K
English (125M)	12	768	12	4	(0.9, 0.95)	50K
Multi (25 M)	3	896	16	4	(0.9, 0.95)	250K

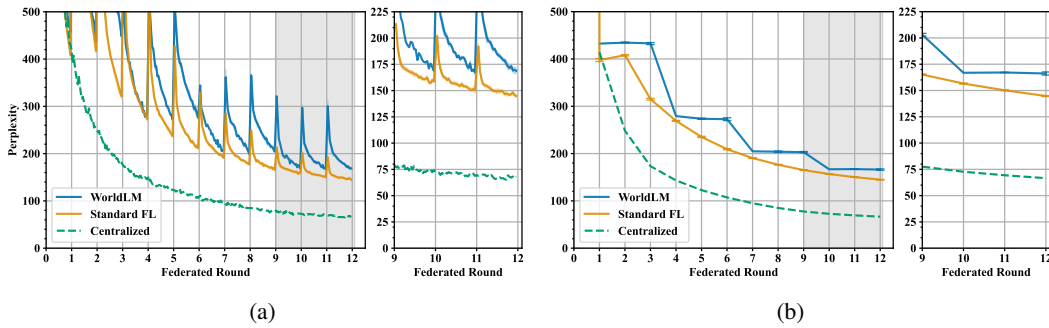


Figure 7: *WorldLM* training (a) and validation (b) performance of the 75M English model on an *IID* partitioning of the C4 dataset. Unlike the results for the heterogeneous partitionings of *The Pile* and *mC4*, *WorldLM* underperforms standard FL as the personalization of attention-based aggregation does not provide benefits. We show a centralized model instead of purely local models, as the *IID* partitioning makes any differences between them minor.

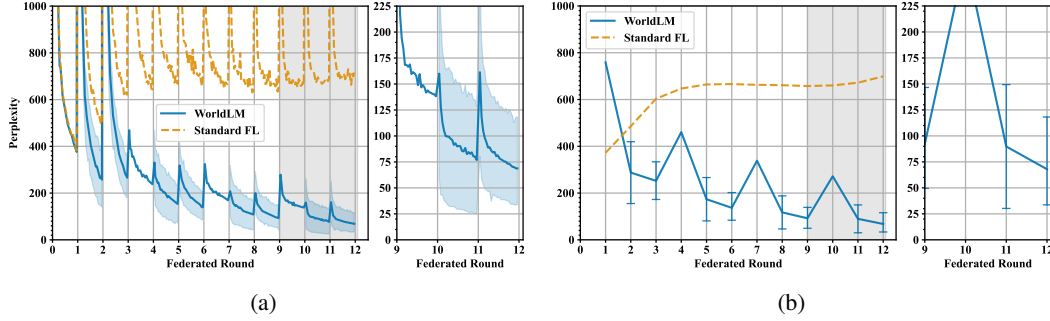


Figure 8: The impact of differential privacy on *WorldLM* performance, with the 75M model on *The Pile*, versus standard FL when using Gaussian noise with  $\sigma = 0.5$  and clipping client pseudo-gradients to the median pre-clip norm of the previous round. *WorldLM* is able to stabilize the training and validation performance (a,b) when applying DP over the leaf **PBC** and **PB** clients, unlike FL which diverges.

## 1 The Legal Context of LLM Training

The surge in popularity of language models, notably exemplified by the release and widespread adoption of ChatGPT, has accelerated the integration of AI into various sectors. This expansion has subsequently encouraged the development of regulatory frameworks to govern AI technologies. A pioneering effort in this domain is the European Union’s Artificial Intelligence Act (the EU AI Act), which represents the first comprehensive legal framework of its kind, anticipated to set a precedent for global AI regulation [76]. The Act encompasses, among various provisions, rigorous data governance guidelines (Art. 10), including adherence to the General Data Protection Regulation (GDPR). This introduces significant challenges for AI developers, particularly concerning the international transfer of data and data de-biasing processes.

*Restrictions in cross-border transfer of data:* The EU’s GDPR imposes stringent conditions on the international transfer of personal data, particularly to third countries deemed to lack adequate protection for personal data. The criterion for ‘adequacy’, as established in *Schrems v DPC* (C-262/14) and Recital 104, requires a level of protection ‘essentially equivalent’ to that of the EU, a high bar for international data transfers, especially to developing countries. Additionally, the requirement for periodic reviews of adequacy for jurisdictions considered equivalent, alongside mandated safeguard measures (Art. 49) for transfers to non-equivalent third countries, introduces a layer of uncertainty and financial burden for businesses engaged in data transfer. Moreover, the EU is not the only jurisdiction tightening controls over data transfer. China, for instance, has enacted laws and supplementary provisions mandating a security assessment by regulator for the transfer of ‘important data’ or personal data exceeding specific thresholds, barring certain exemptions. The varied landscape of regulations poses challenges for accessing diverse local datasets while adhering to disparate, and sometimes significantly different, regulations across jurisdictions. Hierarchical FL offers an efficient solution to maintain compliance by storing data and model within its jurisdiction of origin, avoiding cross-border transfers.

*Mitigation of data bias:* The EU AI Act mandates rigorous oversight throughout the entire lifecycle of the data used in AI models and obligates the implementation of ‘appropriate measures to detect, prevent, and mitigate potential biases’ (Art. 10.2f,fa). It underscores the growing importance of accessing diversified data sources, particularly those from jurisdictions that are underrepresented. To accommodate the acquisition of such data while adhering to individual privacy and local regulations, a novel training paradigm, comprising multiple layers of federation both among clients and jurisdictions, is necessitated to address the limitations of the traditional single-layer FL framework.

*The right to information:* Transparency regarding the data collected and utilized in training, along with the rights of AI developers to access such information, has garnered considerable attention from both regulators and content creators. The GDPR grants individuals the right to obtain all information stored by a service provider (Art. 15, Rec. 63 & 64), including details on the application of this data in training models. Furthermore, the EU AI Act mandates that model providers compile and disclose a comprehensive summary of the training content publicly (Art. 52c). In the US, legal

disputes such as "Times v OpenAI" have underscored the debate over the extent to which the fair use doctrine under US copyright law protects the utilization of copyrighted materials in the training of AI models. This case also ignites broader discussions about the adequacy of the current legal framework in safeguarding content creators against the opaque practices of LLM training. These challenges have led to legislative proposals, including the Generative AI Copyright Disclosure Bill in the US House of Representatives, aimed at enhancing transparency and accountability. Hierarchical FL, by its design, offers inherent advantages over centralized training models by delineating clear data provenance — identifying the sources of data and their contributors. This attribute of Hierarchical FL positions it favorably in addressing concerns related to informational rights and data privacy, presenting a more transparent framework for data utilization in AI development.

*Energy efficiency:* The EU AI Act advocates for the environmentally sustainable development of AI systems by proposing the formulation of a Code of Conduct. This Code is intended to establish explicit objectives and key performance indicators (Art. 69), mirroring the core values of the EU but also responding to growing concerns within the industry and broader society regarding the energy consumption associated with the training and use of AI.