

Reconstruction of Differentially Private Text Sanitization via Large Language Models

Shuchao Pang^{*♣}, Zhigang Lu^{†♣}, Haichen Wang^{*}, Peng Fu[‡], Yongbin Zhou^{*}, Minhui Xue^{§¶}

^{*}Nanjing University of Science and Technology, China

[†]Western Sydney University, Australia

[‡]Institute of Information Engineering, Chinese Academy of Sciences, China

[§]CSIRO's Data61, Australia

[¶]Responsible AI Research (RAIR) Centre, The University of Adelaide, Australia

Abstract—Differential privacy (DP) is the de facto privacy standard against privacy leakage attacks, including many recently discovered ones against large language models (LLMs). However, we discovered that LLMs could reconstruct the altered/removed privacy from given DP-sanitized prompts. We propose two attacks (black-box and white-box) based on the accessibility to LLMs and show that LLMs could connect the pair of DP-sanitized text and the corresponding private training data of LLMs by giving sample text pairs as instructions (in the black-box attacks) or fine-tuning data (in the white-box attacks). To illustrate our findings, we conduct comprehensive experiments on modern LLMs (e.g., LLaMA-2, LLaMA-3, ChatGPT-3.5, ChatGPT-4, ChatGPT-4o, Claude-3, Claude-3.5, OPT, GPT-Neo, GPT-J, Gemma-2, and Pythia) using commonly used datasets (such as WikiMIA, Pile-CC, and Pile-Wiki) against both word-level and sentence-level DP. The experimental results show promising recovery rates, e.g., the black-box attacks against the word-level DP over WikiMIA dataset gave 72.18% on LLaMA-2 (70B), 82.39% on LLaMA-3 (70B), 75.35% on Gemma-2, 91.2% on ChatGPT-4o, and 94.01% on Claude-3.5 (Sonnet). More urgently, this study indicates that these well-known LLMs have emerged as a new security risk for existing DP text sanitization approaches in the current environment.

Index Terms—Large language models, differential privacy, privacy leakage

I. INTRODUCTION

State-of-the-art large language models (LLMs), such as ChatGPT [7] and LLaMA [54], have been applied in numerous real-world applications due to their unprecedented capabilities, achieved through training billions of parameters on vast amounts of text from the Internet [26]. However, several studies [19], [30], [45], [51], [31], [8], [38], [40], [52], [44], [64] have reported privacy leaks due to interactive communication between external users or adversaries and LLMs. For instance, [30], [45], [38] exploit LLMs to extract sensitive information from their training data. Others like [40], [52], [44] demonstrate membership inference attacks (MIAs) against LLMs' training datasets. More recently, [64], [51], [8]

[♣]Shuchao Pang and Zhigang Lu contributed equally. Yongbin Zhou is the corresponding author.

This work is supported by the National Natural Science Foundation of China (Grant No.62206128, No.U2336205), National Key Research and Development Program of China under (Grant No.2023YFB2703900). This work was partially done, when Zhigang Lu was a lecturer with James Cook University. Zhigang Lu is financially supported by Western Sydney University Start-up Funds.

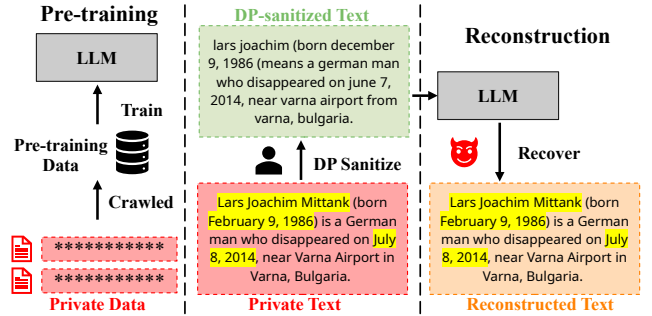


Fig. 1. Overview of reconstruction privacy from given DP-sanitized prompts using LLMs.

show that adversaries can reconstruct original prompts based solely on LLMs' responses.

Unlike existing studies that focus on the “current” privacy issues of LLMs, this paper studies “future” privacy concerns. Our motivation stems from a straightforward yet critical observation: in reality, the boundaries of privacy are not static. Information that was previously in the public domain and used in the training data of LLMs may later become private. For instance, Article 17 of the General Data Protection Regulation (GDPR) specifies the practical circumstance for the *right to be forgotten*, where “The personal data is *no longer necessary* for the purpose an organization originally collected or processed it” [27]. The future needs for privacy preservation require LLMs to provide answers based on up-to-date knowledge, aligning with the latest privacy standards.

A seemingly feasible solution to meet the future privacy needs, without re-training pre-existing LLMs, involves providing differentially private [22] information as the prompts through an interactive retrieval-augmented generation (RAG) process. This allows the LLMs to provide customized responses based on the privacy-preserved information without accessing private details, such as dates, names, numbers, and addresses. More importantly, the randomness of DP, making it a one-way function, further ensures that it is (nearly) impossible to deduce the protected privacy information from the sanitized text (potentially leaked by the prompts leakage attacks). To pre-process/sanitize the original (private) text, we

can either implement the word level DP [25], [24] or the sentence/document level DP [36], [32], [41], [57].

However, in this work, our attacks against DP-sanitization discovered that an adversary can take advantage of the updated LLMs (meeting future privacy needs) to invert non-invertible DP outputs. Specifically, if the private text used during the training of LLMs is then sanitized using DP and fed back to the LLMs as prompts, LLMs can reconstruct the original private information.

To illustrate such a capability, we consider both black-box and white-box adversaries, where the black-box access allows the adversaries to prompt the LLM with a prefix and obtain the probability distribution of the next token via API, whereas the white-box access lets the adversaries learn and modify the model parameters of a given LLM. Based on how we interact with the LLMs, i.e., instruction-based tuning and fine-tuning, we designed two attacks accordingly - black-box instruction-based attacks and white-box fine-tuning-based attacks. In particular, in the black-box instruction-based attacks, we design queries to make instruction-tuned LLMs respond with their memorized content based on the sanitized text for the adversary. In the white-boxed fine-tuning-based attack, the adversary adapts pre-trained LLMs to the reconstruction by fine-tuning it on an auxiliary dataset for a DP text sanitization approach under a specific privacy budget. Note that our attacks can be adapted to any LLM. Fig. 1 depicts an overview of the reconstruction of the private information given DP-sanitized prompts.

We concluded the aforementioned finding against differential privacy by conducting comprehensive experiments on modern LLMs (LLaMA-2, LLaMA-3, ChatGPT-3.5, ChatGPT-4, ChatGPT-4o, Claude-3, Claude-3.5, OPT, GPT-Neo, GPT-J, Gemma-2, and Pythia) using commonly used datasets (WikiMIA, Pile-CC, and Pile-Wiki) against both word-level and sentence-level DP. Our experimental results demonstrated varying levels of success based on model parameters, privacy budgets, and dataset characteristics. For example, let the privacy budget be 12 (which is a commonly used privacy budget in real life to keep the semantics at a reasonable level [17]), the success of reconstruction through the black-box instruction-based attacks against the word-level DP over WikiMIA dataset are 72.18% on LLaMA-2 (70B), 82.39% on LLaMA-3 (70B), 75.35% on Gemma-2, 91.2% on ChatGPT-4o, and 94.01% on Claude-3.5 (Sonnet). Since LLMs do not have long-term memory [58], [16], our findings further argue that the LLMs' ability to reconstruct private information is due to their exposure to the original (unsanitized) data during training, which might have enhanced their precision in recovering certain data.

Our contributions can be summarized as follows.

- We first discover LLMs are capable of reconstructing privacy from differentially private outputs.
- We propose two novel attacks based on the accessibility to large language models - black-box instruction-based attacks against LLMs giving no model parameter access

and white-box fine-tuning-based attacks against LLMs giving model parameter access.

- We provide a novel metric to evaluate the reconstruction attacks on both word level and sentence level sanitization.
- We conduct comprehensive experiments on well-known LLMs and commonly used dataset to show the effects of our attacks against both word-level DP and sentence-level DP.

II. BACKGROUND

This section briefly introduces the existing DP text sanitization approaches and scope of privacy. We give the summary of notations used in this paper in Tab. I and the introduction to language models in Appx. VIII-A.

TABLE I
SUMMARY OF NOTATIONS.

Notation	Definition
\mathcal{T}	Training algorithm
\mathcal{V}	Vocabulary space
\mathcal{X}	Sequence distribution
θ	Model parameters
$X \sim \mathcal{X}$	Sample a pre-training dataset from \mathcal{X}
X_{aux}	Auxiliary dataset for fine-tuning
\mathcal{P}	DP text sanitization approach
\mathcal{P}^{-1}	Reconstruction procedure for DP sanitization mechanism
$\mathbf{x} = \{x_1, \dots, x_n\} \in \mathcal{X}$	Sequence with n tokens in the sequence distribution
$\mathbf{z} \leftarrow \text{CONCATENATE}(\mathbf{x}, \mathbf{y})$	Concatenate sequence \mathbf{x} and \mathbf{y}
$\mathbf{y} \leftarrow \text{GENPROMPT}(\mathbf{p}_T, \mathbf{x})$	Construct prompt using the template \mathbf{p}_T and sequence \mathbf{x}
$\mathbf{x}' \leftarrow \text{GENERATE}(\mathbf{p}, \theta)$	Text generation using the LM with parameter θ for prefix \mathbf{p}
$\tilde{\mathbf{x}} \leftarrow \text{SANITIZE}(\mathbf{x}, \mathcal{P}, \epsilon)$	Text sanitization from private text \mathbf{x} to sanitized text $\tilde{\mathbf{x}}$ using DP text sanitization mechanism \mathcal{P} under privacy budget ϵ
$\hat{\mathbf{x}} \leftarrow \text{RECONSTRUCT}(\tilde{\mathbf{x}}, \mathcal{P}^{-1})$	Text sanitization inversion from sanitized text $\tilde{\mathbf{x}}$ to reconstructed text $\hat{\mathbf{x}}$ using reconstruction attack \mathcal{P}^{-1}

A. Differentially Private Text Sanitization

Differential Privacy [22] (DP) provides privacy guarantees for every single record in a dataset by adding extra noise into query results to limit the influence of each record. In practice, DP has become the de facto standard of privacy definition for machine learning algorithms. Differentially private text sanitization is commonly applied in text anonymization tasks. There are two types of well-established DP text sanitization approaches: word-level DP [25], [24] and document/sentence-level DP [36], [32], [41], [57]. We give the detailed description of the word-level DP and the sentence-level DP in Appx. VIII-B. Alg. 1 and Alg. 2 present the outline of the word- and sentence-level methods, respectively. Tab. II lists the summary of differentially private text sanitization methods.

For texts with different lengths, the word-level DP can not provide privacy guarantees for two texts of the same length because it outputs the fixed-length text. Nevertheless, the sentence-level DP can adapt to texts of varying lengths, with a linear increase in privacy budget as the length of the output text grows. For the privacy definition, based on metric DP,

Algorithm 1 Word-level DP [24].

Input: private text $\mathbf{x} = \{x_1, x_2, \dots, x_n\}$, privacy budget ϵ , pre-trained word embedding model ϕ

Output: sanitized text $\tilde{\mathbf{x}} = \{\tilde{x}_1, \tilde{x}_2, \dots, \tilde{x}_n\}$

- 1: **for** $i \leftarrow 1, 2, \dots, n$ **do**
 - 2: Obtain embedding $\phi_i \leftarrow \phi(x_i)$
 - 3: Sample noise $\mathbf{z} \sim p_\epsilon(\mathbf{z})$
 - 4: Perturb embedding $\tilde{\phi}_i \leftarrow \phi_i + \mathbf{z}$
 - 5: Obtain sanitized word $\tilde{x}_i \leftarrow \operatorname{argmin}_{v \in \mathcal{V}} \|\phi(v) - \tilde{\phi}_i\|$
-

Algorithm 2 Sentence-level DP (based on paraphrasing) [41], [32].

Input: private text \mathbf{x} , temperature T , LM with parameters θ , output length m , prompt template \mathbf{p}_T , clipping constant C , vocabulary \mathcal{V}

Output: sanitized text $\tilde{\mathbf{x}}$

- 1: Construct prompt $\mathbf{y} \leftarrow \text{GENPROMPT}(\mathbf{p}_T, \mathbf{x})$
 - 2: $\mathbf{x}' \leftarrow \emptyset$
 - 3: **for** $i \leftarrow 1, 2, \dots, m$ **do**
 - 4: Compute logit \mathbf{u} with LM using prompt \mathbf{y}
 - 5: Clipping logit $\tilde{\mathbf{u}} \leftarrow \text{CLIP}(\mathbf{u}, C)$
 - 6: Obtain distribution $\mathbb{P} \leftarrow \text{SOFTMAX}(\tilde{\mathbf{u}}, T)$
 - 7: Sample the next token v from \mathcal{V} using \mathbb{P}
 - 8: $\tilde{\mathbf{x}} \leftarrow \tilde{\mathbf{x}} \cup \{v\}$, $\mathbf{y} \leftarrow \mathbf{y} \cup \{v\}$
-

the distance used in the word-level DP mainly reflects word differences within the text but ignores semantic differences. In contrast, the sentence-level DP follows the Local DP (LDP), where any two texts are adjacent, making it hard to achieve a practical privacy budget. For the implementation of DP, the word-level DP introduces perturbation at the word level, and the sentence-level DP perturbs the semantic information of the text. Note that with a small privacy budget, the word-level DP adds a large-scale noise to the embeddings of the original words, significantly changing the word types and resulting in low utility. Tab. III shows an example of the word-level DP (Madlib under $\epsilon = 8$) and the sentence-level DP (DP-Prompt under $T = 2.0$) for text sanitization.

TABLE II

SUMMARY OF DIFFERENTIALLY PRIVATE TEXT SANITIZATION METHODS.

Type	Method	Privacy Definition	Privacy Mechanism
Word-level	MadLib [24]	Metric DP	Laplace
	TEM [20]	Metric DP	Truncated Exponential
Sentence-level	ADePT [36]	LDP	Laplace/Gaussian
	DP-BART [32]	LDP	Laplace/Gaussian
	Paraphraser [41]	LDP	Exponential
	DP-Prompt [57]	LDP	Exponential

B. Personally Identifiable Information

Personally Identifiable Information (PII) refers to any data that can be used to identify a specific individual. PII is crucial for privacy and security, as its misuse can lead to identity theft, financial loss, and privacy violations. Pilán et al. [50] category

PII to direct identifier when one data can re-identify an individual and quasi-identifier when identifiers combined with others can re-identify an individual. This includes direct identifiers like names, phone numbers, and IP addresses, and quasi-identifiers like birth date, gender, and postal code. Named Entity Recognition (NER) is a technology that locates and classifies named entities in text into predefined categories (e.g., names, locations, times). NER is crucial in various natural language processing applications, including search engines, question-answering systems, and content categorization. State-of-the-art NER (e.g., Flair [10], NLTK [14], and SpaCY [28]) classify sequences using a Transformer neural networks. In our case, we leverage NER to tag PII for the given text because it is challenging for a large dataset. In particular, Tab. IV provides the semantics and examples of classes for grouping using NER in our work. Finally, it is noteworthy that in our experiments we did not store any PII as auxiliary knowledge for our attacks.

III. PROBLEM FORMULATION

This section introduces the research question and the threat model, including the attacker’s capabilities and the attack target.

A. Problem Statement

Recall our motivating example of the “future” privacy issues in Sec. I. Since the scope of privacy might not be fixed, portions of the training data used for existing LLMs could potentially become private in the future, even if they were not initially considered as such.

Among all privacy enhance techniques, differential privacy (DP) [22] is an ideal solution to address such “future” privacy issues by using DP-sanitized text as prompts to update the knowledge base of a trained LLM. This allows the updated LLM to use the privacy-preserved knowledge instead of the original private information when answering external requests. Thanks to the rigorous privacy guarantee provided by DP, the existing prompts leakage attacks [64], [51], [8] can only reveal the DP-sanitized prompts but not the original ones.

Nevertheless, take a reasonable assumption where the DP-sanitized prompts should have similar semantics to the original text, a question remains open: *In our future privacy circumstance, given DP-sanitized prompts, could LLMs recover the original privacy of the sanitized prompts?*

B. Threat Model

Adversary’s Capabilities. We consider that adversaries either have black-box or white-box access to trained LLMs. For black-box access, an adversary can prompt the LLM with a prefix and obtain the probability distribution of the next token via paid APIs, e.g., ChatGPT and Claude; whereas the white-box adversaries have an auxiliary dataset following the same distribution as the private training dataset and the access to modify the model parameter θ of the target LLMs, such as OPT, Pythia, GPT-Neo and GPT-J. We further assume that the same as other DP approaches, the DP-sanitized prompts,

TABLE III
EXAMPLE OF THE WORD-LEVEL DP AND THE SENTENCE-LEVEL DP.

Type	Example
Original	Well, I'm Tony. I live in Taichung, Taiwan, but I come from Nova Scotia, Canada. Like most expatriates here, I teach English to pay the bills. I'm married to a Taiwanese woman and plan on staying here. I started gaming around the time the Wilderness Survival Guide was released.
Word-level	making, i'm tony has i live in taichung, taiwan, but know want from nova scotia met canada. like ever expatriates here, i teach english it pay in cards and my'm married then a taiwanese babies it plan on anxious informed end i started gaming watch sense times vast wilderness aiming guide although released alone
Sentence-level	Taiwan, but I originally hail from Nova Scotia, Canada. Similar to many foreigners here, I earn income by teaching the English language. I am happily married to a Taiwanese national and intend to establish permanent residence in Taichung. I began my gaming hobby during the time when the Wilderness Survival Guide was newly published.

TABLE IV
SEMANTICS AND EXAMPLES OF PII CLASSES.

Name	Semantics	Examples
cardinal	cardinal value	181
date	date value	2014
event	event name	Hurricane Ana
fac	building name	the Stade de France
gpe	geo-political entity	Egypt
language	language name	Spanish
law	law name	The Local Audit and Accountability Act 2014
loc	location name	the Central Pacific
money	money name	€375
norp	affiliation	Conservatives
ordinal	ordinal value	second
org	organization name	Muslim Brotherhood
percent	percent value	42.1%
person	person name	Mohamed Badie
product	product name	Ziyuan I-04
quantity	quantity name	82 metres
time	time value	2:02:57
work of art	name of work of art	The BRW Rich 200, 2014

the privacy budget and the DP approach (word-level DP or sentence-level DP) are publicly available [12]. Note that the difference between the DP-sanitized text and the original text is determined by the privacy budget and the DP approach.

Adversary's Target. The adversaries aim to generate a reconstructed version of the original text corresponding to the DP-sanitized text. Prior work [18] shows that only 1% of the pre-training dataset is memorized by some LLMs, indicating that generating verbatim memorization for LLMs directly is challenging. Therefore, compared with the previous works [45], [18] that focus on memorization of the pre-training dataset in LLMs, our goal is to investigate how to generate sensitive information rather than the verbatim sequence in the training data.

Definition 1 (Reconstruction). *Let a language model having model parameters θ be trained on X . Given a text $x \in X$ and its DP-sanitized copy \tilde{x} , the x is reconstructable if $\text{GENERATE}(p, \theta) = x$, where p is the attacking prompt constructed by \tilde{x} .*

IV. METHODOLOGY

In this section, we give the technical details of our reconstruction attacks against the DP sanitization, given black-box access or white-box access to the LLMs, respectively.

A. Overview

In a nutshell, the two attacks, black-box instruction-based attacks and white-box fine-tuning-based attacks, contains the following four constructing blocks, which covers the functionalities of LLMs (GENERATE) and text processing operations (GENPROMPT, CONCATENATE, and SANITIZE). Specifically, the key idea behind our attacks is to use pairs of example text and its DP-sanitized copy to trigger the memorization of the target LLM, so that LLM could return the private text for given DP-sanitized prompts. Alg. 3 depicts our two attacks from Line 1 and Line 5, respectively.

- $\text{GENERATE}(p, \theta)$: Given prompt p and a trained LLM's model parameter θ , the model returns the answer. With black-box access to the model, we can utilize APIs to generate the response.
- $\text{GENPROMPT}(p_T, x)$: For a given sequence x and prompt template p_T , generate a new prompt.
- $\text{CONCATENATE}(x, y)$: For two sequences x and y , generate a new sequence by concatenating them.
- $\text{SANITIZE}(x, \mathcal{P}, \epsilon)$: For a given text x , return sanitized text by applying DP text sanitization approach \mathcal{P} under the privacy budget ϵ .

B. Black-box Instruction-based Attacks

Instruction-tuned LLMs can be applied to various tasks by following (human) instructions. This is because they have been fine-tuned on extensive data of instructional questions and corresponding answers for dialogue scenarios. Consequently, we can leverage the instruction-following capabilities of these models to perform reconstruction attacks. Specifically, we propose an attack based on instructions for instruction-tuned LLMs, which reconstructs sanitized text by querying the model with a specific prompt. Line 1 to Line 4 in Alg. 3 presents the formal workflow of the black-box instruction-based attack. As shown in Fig. 2(a), for the target sanitize text \tilde{x} and a instruction-tuned LLM with model parameter θ , we assume that an adversary has the black-box access to the model. First,

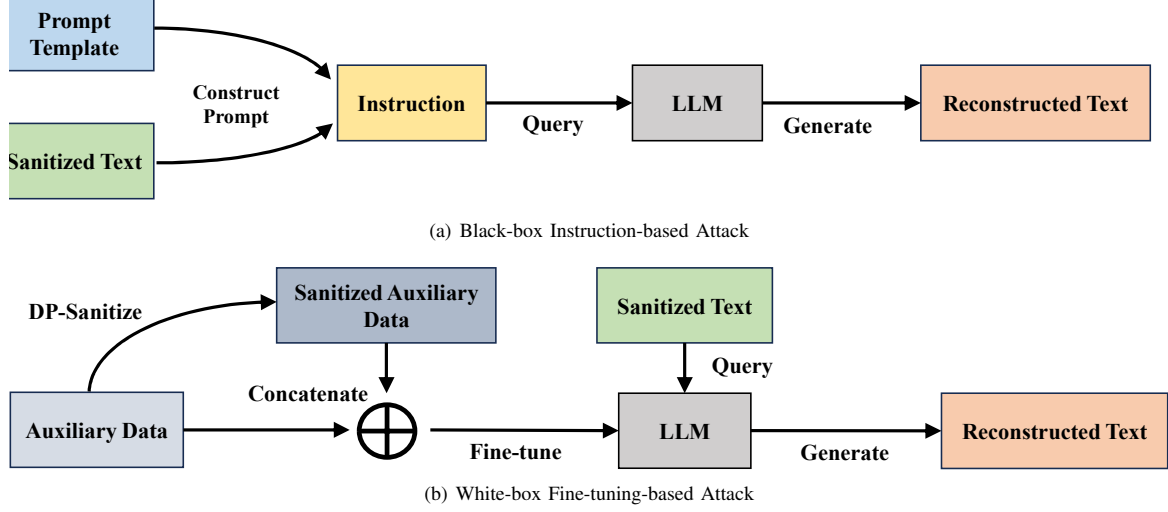


Fig. 2. Overview of the reconstruction attacks against the DP text sanitization.

Algorithm 3 Reconstruction Attacks

Input: target sanitized text \tilde{x} , LLM with parameter θ , prompt template p_T , auxiliary dataset X_{aux} , DP text sanitization approach \mathcal{P} under privacy budget ϵ

Output: reconstructed text \hat{x}

```

1: function INSTRUCTIONATTACK( $\tilde{x}, p_T, \theta$ )
2:   Construct instruction  $p \leftarrow \text{GENPROMPT}(p_T, \tilde{x})$ 
3:   Query model  $\hat{x} \leftarrow \text{GENERATE}(p, \theta)$ 
4:   return  $\hat{x}$ 
5: function FINETUNINGATTACK( $\tilde{x}, X_{\text{aux}}, \mathcal{P}, \epsilon, \theta$ )
6:   repeat
7:     Sample data from public dataset  $y \sim X_{\text{aux}}$ 
8:     Sanitize data  $\tilde{y} \leftarrow \text{SANITIZE}(y, \mathcal{P}, \epsilon)$ 
9:      $z = \{z_i\} \leftarrow \text{CONCATENATE}(\tilde{y}, y)$ 
10:    Calculate loss
        
$$L \leftarrow - \sum_i \log \Pr(z_i | z_1, z_2, \dots, z_{i-1}; \theta)$$

11:    Update  $\theta$  by taking gradient descent on  $\nabla_{\theta} L$ 
12:  until convergence
13:  Query model  $\hat{x} \leftarrow \text{GENERATE}(\tilde{x}, \theta)$ 
14:  return  $\hat{x}$ 

```

the adversary prepares a prompt template p_T as blow where the $\{\text{original text}\}$ is the private text and the $\{\text{edited text}\}$ is the DP-sanitized text.

You are a helpful assistant who can help users generate the original text based on the edited text, and you may have seen the original text. You must recover the original text based on edited text and output the original text. For example, you have known $\{\text{original text}\}$, for a user prompt with $\{\text{edited text}\}$, you should only output the $\{\text{original text}\}$ directly.

Demonstration
User: $\{\text{edited text}\}$
Assistant: $\{\text{original text}\}$

Then, the adversary constructs instructions using the prompt template p_T and sanitized text \tilde{x} . Finally, the adversary inputs the instruction into the model and uses the output as reconstructed text corresponding to the sanitized text. The prompt template aims to enable LLMs to respond with content related to sanitized text based on the previous training. This attack method is simple yet efficient, and we discover it can recover a significant amount of original text under commonly used privacy budgets (e.g., $\epsilon = \{8, 12\}$). See the detailed experimental results in Sec. V.

C. White-box Fine-tuning-based Attacks

When given white-box access to an LLM, adversaries could do much more than using instructions to impact the behaviors of LLMs. Intuitively, adversaries fine-tune the target LLMs using structured pairs of original text and DP-sanitized text, then guide the LLMs to return the private text based on given DP ones. Line 5 to Line 14 in Alg. 3 and Fig. 2(b) provide the workflow of the white-box fine-tuning-based attack, where adversaries know a target DP-sanitized text \tilde{x} , an auxiliary dataset X_{aux} , the DP text sanitization approach \mathcal{P} , the privacy budget ϵ , and a pre-trained LLM with parameter θ . The adversary samples the data point y from the auxiliary dataset, following the same distribution as the target training dataset, and constructs a new sequence z by concatenating the DP-sanitized text $\tilde{y} = \text{SANITIZE}(y, \mathcal{P}, \epsilon)$ using privacy budget ϵ and original text y as $z = \text{CONCATENATE}(\tilde{y}, y)$. Then, the adversary fine-tunes the model using the following objective:

$$\mathcal{L}(\theta) = - \sum_i \log \Pr(z_i | z_1, z_2, \dots, z_{i-1}; \theta), \quad (1)$$

where z_i is each token in z . After the fine-tuning process, the adversary inputs the sanitized prompts into the model and uses the output as reconstructed text corresponding to the sanitized text. The goal of fine-tuning is to make the model learn the pattern from the sanitized text to the original text. In practice, following previous works on fine-tuning LLMs for paraphrasing [60], we separate the sanitized text \tilde{y} and original text y when constructing z .

V. EXPERIMENTAL EVALUATION

In this section, we evaluate our attacks, the black-box instruction-based attacks and the white-box fine-tuning-based attacks, on the real world datasets and the latest applications of LLMs against two famous DP implementations, the word-level DP [24] and the sentence-level DP [57].

A. Large Language Models

In this work, based on how the adversaries could interact with the LLMs, we categorize the LLMs into two types - the LLMs only accepted external instructions (targets of the black-box attacks) and the LLMs were further fine-tuned by given datasets (targets of the white-box attacks). Tab. V gives the summary of LLMs used in our experiments, including the model size, model version, and the accessibilities to the model parameters and the training datasets, where “Y” and “N” indicate accessible or inaccessible, respectively. Appx. VIII-C shows the details of the LLMs in our experiments.

B. Datasets

To evaluate the performance of our attacks, we should have the training data of the LLMs as the ground truth. However, limited by the intellectual property, such information is not publicly available for those LLMs being the targets of our black-box attacks (e.g., LLaMA and ChatGPT). Hence, following existing studies [52], we also assume that WikiMIA is part of the training data used by those LLMs. For the LLMs being attacked by the white-box attacks, since they are open-sourced, we use their training dataset directly in the experiments. Tab. VI provides the statistics for the datasets we used. Note that we follow the existing works [38], [52] to truncate the original data into specific lengths. The details of the datasets are as follows.

- **WikiMIA [52]** was created by Shi et al., where the data is crawled from the recent event pages from Wikipedia. Specifically, for models released from 2017 to 2023, they consider the events after 2023 as non-members of pre-training data and the events before 2017 as members of pre-training data.
- **Pile [26]** is an 825 GB dataset, which has been used to pre-train several language models (e.g., OPT, GPT-Neo, GPT-J). In our experiments, we select subsets of Pile-CC, Pile-Wiki, and Pile-Enron, which contain the data crawled from public web pages by Common Crawl, Wikipedia content, and Enron Email Dataset [35] in Pile, respectively. For each subset, we randomly select 10,000 records. Note that, since Pile was deleted from

the official server [5] due to the copyrighted content, we leverage an uncopyrighted version [6] rather than the official version, where the data from subsets of Books3, BookCorpus2, OpenSubtitles, YTSUBtitles, and OWT2 subsets have been removed.

C. Differentially Private Text Sanitization Approaches

In the experiments, we choose MadLib [25] (Alg. 1) as the word-level DP in our experiments, since this is the commonly used DP word-level implementation [41], [20]. In MadLib, the distance function is defined in Euclidean space and Laplace noise is added to the word embedding vector. We choose DP-Prompt [57] (Alg. 2) as the sentence-level DP in our experiments, since Utpala et al. [57] demonstrate the DP-Prompt achieves better utility compared to other approaches when using ChatGPT. In DP-Prompt, we consider using ChatGPT-3.5 as base model to generate the paraphrased text.

D. Metrics

To measure the effectiveness of the reconstruction attacks, we consider the following evaluation metrics for privacy extraction.

- **RECALL and PRECISION.** In our study, we focus on the privacy leakage of sensitive content in the text rather than the shared vocabulary (e.g., time, addresses, and names), which are more prone to causing privacy concerns; whereas common words like “the” and “this” do not lead to privacy issues. That is, we aim to recover the privacy-sensitive content from the original text. Hence, we extract and mark PII sequences (see Sec. II for details) from the text and consider these sequences as the privacy within the given text. Formally, we denote the set of PII sequences in the original text x as C , in the DP-sanitized text \tilde{x} as \tilde{C} , and in the reconstructed text \hat{x} as \hat{C} . We define RECALL and PRECISION for the reconstruction attacks below.

$$\text{RECALL} = \mathbb{E} \left[\frac{|C \cap \hat{C} - \tilde{C}|}{|C - \tilde{C}|} \right], \quad (2)$$

$$\text{PRECISION} = \mathbb{E} \left[\frac{|C \cap \hat{C} - \tilde{C}|}{|\hat{C} - \tilde{C}|} \right]. \quad (3)$$

In Equations (2) and (3), $|C \cap \hat{C} - \tilde{C}|$ represents the number of PII sequences that match in the original text but are missing in the sanitized text. $|C - \tilde{C}|$ represents the number of PII sequences present in the original text but missing in sanitized text. $|\hat{C} - \tilde{C}|$ denotes the number of PII sequences present in the reconstructed text but missing in the sanitized text.

- **SUCC.** We define the success of reconstruction based on extracted PII sequences. Specifically, if any PII sequence that is extracted from the reconstructed text matches the original text, we consider the extraction to be successful. Formally, for each original text x and reconstructed

TABLE V
SUMMARY OF MODELS.

Operation	Model	Size / Version	Weight Access	Dataset Access
Instruction	LLaMA-2	7B, 13B, 70B	Y	N
	LLaMA-3	8B, 70B	Y	N
	Gemma-2	9B, 27B	Y	N
	ChatGPT-3.5	gpt-3.5-turbo-0125	N	N
	ChatGPT-4	gpt-4-turbo-2024-04-09	N	N
	ChatGPT-4o	gpt-4o-2024-05-13	N	N
	Claude-3 (Haiku)	claude-3-haiku-20240307	N	N
	Claude-3 (Sonnet)	claude-3-sonnet-20240229	N	N
	Claude-3 (Opus)	claude-3-opus-20240229	N	N
Fine-tuned	Claude-3.5 (Sonnet)	claude-3-5-sonnet-20240620	N	N
	OPT	350M, 1.3B, 6.7B	Y	Y
	GPT-Neo, GPT-J	1.3B, 2.7B, 6B	Y	Y
	Pythia	350M, 1.3B, 6.7B	Y	Y

TABLE VI
SUMMARY OF DATASETS.

Name	Length	Records	Pre-training data for Models
WikiMIA	64	284	LLaMA, ChatGPT, Claude
Pile-CC	64	10000	OPT, GPT-Neo, GPT-J, Pythia
Pile-Wiki	64	10000	OPT, GPT-Neo, GPT-J, Pythia
Pile-Enron	64	10000	OPT, GPT-Neo, GPT-J, Pythia

TABLE VII
PROMPT TEMPLATE USED TO QUERY CHATGPT TO OBTAIN THE SCORES.

System	Assume you are a helpful assistant. Your task is to analyze the match rate of the key information (e.g., time, place, person) in two documents. Based on your assessment, assign the response a numerical score ranging from 0 (low similarity) to 10 (high similarity). [Example] User: Text1: {text1} Text2: {text2} Assistant: {score}
User	Text1: {text1} Text2: {text2}

text \hat{x} , the successful reconstruction SUCC is defined as follows:

$$\text{SUCC}(x, \hat{x}) = \mathbb{1}[C \cap \hat{C} - \tilde{C} \neq \emptyset]. \quad (4)$$

- **SCORE.** For some exceptional cases, previous metrics may incur inaccurate results. For example, consider that “8 July 2014” is changed to “2014 July 8” during DP text sanitization (e.g., paraphrase-based method). However, they are considered different PII sequences, yet they have the same meaning. Following the prior works of jail-breaking attacks on LLMs, we leverage LLMs as the evaluator to measure the similarity of sensitive information between the sanitized text and the original text. Specifically, we prompt ChatGPT with the sanitized text and original text, and ChatGPT reports the quality of our reconstruction attacks, which is rated from 1 (low quality) to 10 (high quality). We define this Metrics as SCORE.

E. Implementation

To tag PII sequences from text, we leverage Flair [10] as the PII extraction model released in HuggingFace [2]. Specifically, Flair is a NER framework based on Transformer networks to classify tokens as PII sequences. It is noteworthy that in our experiments we did not store any PII as auxiliary knowledge for our attacks. For the models giving weight access (e.g. LLaMA, Gemma and OPT), we downloaded checkpoints from HuggingFace. For the models not giving weight access (e.g. ChatGPT, Claude), we query models via black-box APIs available online (e.g., OpenAI API [4] and Anthropic AI API [1]). For DP text sanitization approaches, we implement both the word-level DP and the sentence-level DP based on DP-Prompt repository [56]. Note that we implement the word-level DP using 50-dimensional GloVe [49] vectors (following existing works [41], [57]) as word embeddings. We implement our reconstruction attacks based on PyTorch [47] and Transformers [61]. To fine-tune the pre-trained LLMs, we leverage LoRA [29] based on PEFT [39] library, a parameter-efficient fine-tuning method, to reduce the trainable parameters due to the limited computational resource. To obtain the sensitive information similarity by LLMs, we employ ChatGPT-3.5 as the base model. Tab. VII presents the prompt templates used for evaluating the sensitive information similarity. Finally, we run all the experiments on a GPU cluster, which is equipped with NVIDIA RTX3090, RTX4090 and A800.

F. Results of Black-box Instruction-based Attacks

Setup. To evaluate the effectiveness of the black-box instruction-based attack, we conduct experiments on WikiMIA using both the word-level DP and the sentence-level DP under various privacy budgets ($\epsilon = \{4, 8, 12\}$ for the word-level DP [24] or $T = \{2.0, 1.5, 1.0\}$ for the sentence level DP [57], where the relationship between T and the privacy budget can be found in Sec. II) with instruction-tuned LLMs, including LLaMA, Gemma, ChatGPT, and Claude. We adjust the prompt per Fig. 2 for different models and query models with the sanitized text.

Results. Tab. VIII and Tab. IX provides an example of the black-box instruction-based attack on WikiMIA under

TABLE VIII
EXAMPLE OF THE BLACK-BOX INSTRUCTION-BASED ATTACKS AGAINST THE WORD-LEVEL DP ON WIKIMIA.

	WikiMIA
Original	The Eurovision Song Contest 2014 was the 59th edition of the Eurovision Song Contest. It took place in Copenhagen, Denmark, following the country's victory at the 2013 contest with the song "Only Teardrops" by Emmelie de Forest. Organised by the European Broadcasting Union (EBU) and host broadcaster Danish Broadcasting Corporation (DR), the contest was held at B&W Hallerne, and consisted of two semi-finals on
DP-sanitized (Madlib, $\epsilon = 8$)	head eurovision song ecuadorian 2014 being the 31st page freedom itself eurovision song lottery open entire took summer city lewisham river netherlands above planned branch warn's victory center upon 2013 contest apart third soundtrack "episode three-inch ". de lands afterwards organised by push international broadcasting union) jtrs respectively and newcomer broadcaster danish producer corporation m abul), end contest was held at c hip stripe, similar consisted northern seven semi-finals.
Reconstructed (ChatGPT-4)	The 2014 Eurovision Song Contest, the 59th edition of the annual event, was held in Copenhagen, Denmark. It took place at the B&W Hallerne, following Denmark's victory at the 2013 contest with the song "Only Teardrops" by Emmelie de Forest. The event was organised by the European Broadcasting Union (EBU) and host broadcaster Danmarks Radio (DR). The contest consisted of two semi-finals and a final, which were held in May 2014
Reconstructed (Claude-3-Opus)	The Eurovision Song Contest 2014 was the 59th edition of the annual Eurovision Song Contest. It took place in Copenhagen, Denmark, following Emmelie de Forest's win at the 2013 contest in Malmö, Sweden with the song "Only Teardrops". It was the third time Denmark had hosted the contest, the most recent previous occasion being in 2001. Danish public broadcaster DR organised the contest at B&W Hallerne, with the two semi-finals held on 6 and 8 May, and the final held on 10 May 2014. The three live shows were presented by Lise Rønne, Nikolaj Koppel and Pilou Asbæk.
Reconstructed (LLaMA-3-70B)	The Eurovision Song Contest (ESC) 2014 was the 59th edition of the annual Eurovision Song Contest, held in Copenhagen, Denmark, after Danish singer Emmelie de Forest won the ESC the year before. The contest consisted of two semi-finals, which took place on 6 May and 8 May 2014, and the final on 10 May 2014. The shows were hosted by Lise Rønne, Nikolaj Koppel, Pilou Asbæk, and Josh Dubovie. Ten countries participated in each semi-final,
Reconstructed (Gemma-2-27B)	The Eurovision Song Contest 2014 was the 59th edition of the annual Eurovision Song Contest. It was held in Copenhagen, Denmark, following Emmelie de Forest's win at the 2013 contest in Malmö, Sweden with the song "Only Teardrops". The event took place at the B&

$\epsilon = 8$ using ChatGPT-4, Claude-3-Opus, LLaMA-3-70B and Gemma-2-27B for the word-level DP and the sentence-level DP, respectively. The original text x , sanitized text \tilde{x} and reconstructed text \hat{x} are listed, where the highlighted text is PII sequences extracted by the NER model, and the text in the red box contains the PII sequences that remain unchanged. For word-level DP, we observe that the reconstructed text can correct the errors in the sanitized text (e.g., reconstructed text using ChatGPT-4 correct "31st" to "51st"). Compared to word-level DP, sentence-level DP retains most of the PII sequences from the original text, thereby fewer PII sequences are successfully reconstructed.

The numeric results on WikiMIA for the word-level DP are detailed in Tab. X and Tab. XI, respectively. For the word-level DP, in a practical privacy budgets (e.g., $\epsilon = 8$ and $\epsilon = 12$), the black-box instruction-based attacks successfully reconstruct sensitive information at the word level with high probability. Nevertheless, the black-box instruction-based attacks have no significant effect under a smaller privacy budget due to substantial discrepancies between the original and sanitized texts. For the sentence-level DP, we observe that SUCC, RECALL, and PRECISION are lower than the word-level DP, but SCORE is higher. The reason behind it is in two folds. First, the sentence-level DP fails to remove the sensitive information (see examples as the text enclosed in the red boxes in Tab. XI). Second, the metrics of RECALL, PRECISION, and SUCC measures the difference between the DP-sanitized text and the reconstructed text. Hence, these three metrics do not

show a promising results.

For models (e.g., LLaMA and Gemma) giving weight access, which, however, were not used in the black-box attacks, we observe that the black-box instruction-based attack performs better on larger models (e.g., LLaMA-2 with 70B parameters achieves higher SUCC, RECALL, PRECISION, and SCORE than the version with 7B and 13B parameters, and Gemma-2 with 27B parameters also achieves a higher SUCC, RECALL, PRECISION, and SCORE than the version with 9B parameters). For non-open-source models, our attacks perform better on newer models (e.g., ChatGPT-4 achieves a higher SUCC than ChatGPT-3.5). Note that, for sentence-level DP, although our attacks cannot reconstruct correct semantic construction, they can still recover some PII sequences present in the original text. For evaluation of SCORE, We observe that SCORE also increases with the number of model parameters or the model query cost. Note that the results on LLaMA-2 (7B) outperform LLaMA-2 (13B), this is probably because the prompt performs poorly with the given prompt. Additionally, some discussions on online forums [3] show that LLaMA-2 (13B) is performing worse than LLaMA-2 (7B) in terms of some specific metrics.

G. Results of White-box Fine-tuning-based Attacks

Setup. To evaluate the effectiveness of the white-box fine-tuning attacks on the pre-trained LLMs, we conduct experiments on Pile-CC, Pile-Wiki, and Pile-Enron with pre-trained LLMs, including OPT, Pythia, GPT-Neo and GPT-J.

TABLE IX
EXAMPLE OF THE BLACK-BOX INSTRUCTION-BASED ATTACKS AGAINST THE SENTENCE-LEVEL DP ON WIKIMIA.

	WikiMIA
Original	The Eurovision Song Contest 2014 was the 59th edition of the Eurovision Song Contest. It took place in Copenhagen, Denmark, following the country's victory at the 2013 contest with the song "Only Teardrops" by Emmelie de Forest. Organised by the European Broadcasting Union (EBU) and host broadcaster Danish Broadcasting Corporation (DR), the contest was held at B&W Hallerne, and consisted of two semi-finals on
DP-sanitized (DP-Prompt, $T = 1.5$)	The 2014 Eurovision Song Contest was the 59th installment of the contest and was held in Copenhagen, Denmark. This was because Denmark won the previous year's contest with the song "Only Teardrops" by Emmelie de Forest. The contest was organized by the European Broadcasting Union and hosted by the Danish Broadcasting Corporation. It took place at B&W Hallerne and consisted of two semifinals.
Reconstructed (ChatGPT-4)	The 2014 Eurovision Song Contest was the 59th edition of the annual Eurovision Song Contest. It took place in Copenhagen, Denmark, following Emmelie de Forest's win at the 2013 contest in Malmö, Sweden with the song "Only Teardrops". The event was organised by the European Broadcasting Union (EBU) and host broadcaster DR. The contest was held at B&W Hallerne and consisted of two semi-finals and a final.
Reconstructed (Claude-3-Opus)	The 2014 Eurovision Song Contest was the 59th edition of the Eurovision Song Contest. It took place in Copenhagen, Denmark, following Emmelie de Forest's win at the 2013 contest in Malmö, Sweden with the song "Only Teardrops". It was the third time that Denmark hosted the contest, the most recent previous occasion being in 2001. Danish public broadcaster DR organised the event, choosing the B&W Hallerne as the host venue after considering several bids from cities and venues across Denmark. The contest consisted of two semi-finals on 6 and 8 May, and the final on 10 May 2014.
Reconstructed (LLaMA-3-70B)	The 2013 Eurovision Song Contest was the 1989 installment of the contest and was held in Malmö, Sweden. This was because Loreen from Sweden won the previous year's contest with the song 'Euphoria'. The contest was organized by the European Broadcasting Union (EBU) and hosted by Sveriges Television (SVT). It took place at Malmö Arena and consisted of two semi-finals.
Reconstructed (Gemma-2-27B)	The 2014 Eurovision Song Contest was the 59th edition of the annual competition and took place in Copenhagen, Denmark. Denmark earned the right to host after their victory in the 2013 contest with the song "Only Teardrops", performed by Emmelie de Forest.

Specifically, for each dataset, we randomly select a subset containing 10,000 samples from the original datasets and split the subset into a training set having 8,000 samples, a validation set having 1,000 samples, and a test set having 1,000 samples. We fine-tune the pre-trained LLMs using the training set and the validation set and evaluate on the test set. Due to the high costs incurred by the sentence-level DP when querying the black-box API, we consider performing the fine-tuning attack for the word-level DP only.

Results. Tab. XV provides an example of the white-box fine-tuning-based attacks on Pile-CC under $\epsilon = 8$ with Pythia-6.9B, OPT-6.7B and GPT-J-6B for the word-level DP. We observe that, the open-source model reconstructs few PII sequences compared to close-source models (e.g., ChatGPT, Claude).

Tab. XII, Tab. XIII, and Tab. XIV report the reconstruction results and PRECISION on Pile-CC, Pile-Wiki and Pile-Enron, respectively, where the metrics include SUCC, RECALL and PRECISION. Similar to the black-box instruction-based attacks, we observe that the model with more parameters can achieve higher performance metrics. For Pile-CC, the metrics including SUCC, RECALL, and PRECISION are lower than Pile-Wiki

and Pile-Enron, this may be because Pile-CC is not composed of a specific type of data. Therefore, the model cannot learn from a specific data distribution like fact (Pile-Wiki) or email (Pile-Enron) distribution.

H. Ablation Studies

The original text of the DP-sanitized one was not seen by LLMs. Tab. XVI shows the results of prompting fine-tuned white-box LLMs with DP-sanitized text, where the original text was not seen by the LLMs. From the results, we can see that the LLMs we used still achieve acceptable recovery outcome compared to the cases where the original text of the DP-sanitized ones was seen by LLMs.

Privacy budgets. In this experiment, we aim to investigate how privacy budget affects the quality of reconstruction attacks. Intuitively, privacy budgets control the level of modification for the DP text sanitization approach. For experimental settings, we vary the privacy budget from 1 to 32 and apply the black-box instruction-based attack to LLaMA models. Fig. 3(a), Fig. 3(b), Fig. 3(c) respectively provide the correlation between the SUCC, RECALL, PRECISION, and the privacy budget. We can observe that, for a greater privacy budget

TABLE X
RESULTS OF THE BLACK-BOX INSTRUCTION-BASED ATTACKS AGAINST THE WORD-LEVEL DP ON WIKIMIA.

Models	$\epsilon = 12$				$\epsilon = 8$				$\epsilon = 4$			
	SUCC	RECALL	PREC	SCORE	SUCC	RECALL	PREC	SCORE	SUCC	RECALL	PREC	SCORE
LLaMA-2-7B	62.68	18.21	27.45	5.61	38.38	6.76	12.73	2.35	3.52	0.36	0.86	0.82
LLaMA-2-13B	53.52	16.22	24.96	5.12	18.31	3.52	6.30	2.29	1.06	0.11	0.31	1.37
LLaMA-2-70B	72.18	23.05	32.28	6.32	44.01	7.97	13.91	3.01	3.52	0.32	1.28	0.92
LLaMA-3-8B	68.31	20.47	19.58	6.89	51.06	10.01	12.26	4.38	8.10	0.86	1.27	1.08
LLaMA-3-70B	82.39	31.61	30.72	7.37	59.51	12.48	12.87	4.16	5.99	0.64	0.69	0.87
Gemma-2-9B	70.77	20.87	35.80	6.64	45.07	8.96	15.49	4.23	0.00	0.00	0.00	1.54
Gemma-2-27B	75.35	24.63	39.22	7.20	54.93	11.54	18.12	4.68	0.35	0.03	0.06	2.68
ChatGPT-3.5	80.99	31.59	45.10	7.21	62.32	14.41	22.50	3.71	6.69	0.66	0.71	0.48
ChatGPT-4	88.38	45.09	53.40	8.55	67.96	17.54	31.52	6.14	5.63	0.56	1.33	0.80
ChatGPT-4o	91.20	46.61	56.17	8.35	65.49	16.70	22.15	4.22	6.34	0.68	0.77	0.53
Claude-3-Haiku	64.44	23.75	36.45	7.08	50.00	10.64	22.77	4.43	4.93	0.49	0.60	0.95
Claude-3-Sonnet	85.92	36.31	42.82	7.71	58.10	16.07	20.55	4.86	4.93	0.59	0.76	0.75
Claude-3-Opus	92.96	56.73	51.71	8.78	78.87	29.33	21.25	6.89	11.97	1.48	0.79	0.88
Claude-3.5-Sonnet	94.01	56.41	54.70	8.73	77.11	26.81	29.60	7.15	9.15	1.03	2.21	0.75

TABLE XI
RESULTS OF THE BLACK-BOX INSTRUCTION-BASED ATTACKS AGAINST THE SENTENCE-LEVEL DP ON WIKIMIA.

Models	$T = 1.0$				$T = 1.5$				$T = 2.0$			
	SUCC	RECALL	PREC	SCORE	SUCC	RECALL	PREC	SCORE	SUCC	RECALL	PREC	SCORE
LLaMA-2-7B	6.69	2.34	4.68	9.01	6.69	2.16	5.05	8.92	5.63	2.04	4.25	9.13
LLaMA-2-13B	12.32	5.18	6.23	6.98	13.03	4.02	7.16	7.14	11.62	5.20	6.24	7.41
LLaMA-2-70B	13.03	4.81	7.55	9.10	16.20	5.31	9.85	9.06	13.03	5.35	8.87	9.27
LLaMA-3-8B	12.32	5.09	3.50	7.54	16.55	5.46	4.44	7.47	10.56	3.73	3.09	7.58
LLaMA-3-70B	16.55	6.46	5.92	7.89	27.82	10.28	7.04	8.32	15.85	6.56	4.16	8.45
Gemma-2-9B	17.25	6.52	9.82	9.00	17.96	5.92	10.03	9.04	13.03	4.72	7.69	9.01
Gemma-2-27B	23.24	8.87	12.35	8.60	21.48	7.53	11.21	8.72	19.72	8.53	10.56	8.63
ChatGPT-3.5	9.15	3.48	6.16	9.58	11.97	4.49	9.27	9.54	7.39	3.91	6.25	9.71
ChatGPT-4	20.42	8.38	11.75	9.26	26.41	10.14	15.33	9.24	19.37	8.74	10.95	9.24
ChatGPT-4o	8.80	4.13	5.42	9.42	14.08	5.08	9.47	9.45	11.27	5.03	7.88	9.47
Claude-3-Haiku	4.93	1.80	3.70	8.93	7.04	2.39	4.74	9.01	5.28	1.91	3.81	9.12
Claude-3-Sonnet	23.24	10.30	12.33	9.12	23.24	9.40	11.92	9.16	22.18	11.19	9.48	9.04
Claude-3-Opus	30.63	14.57	14.55	9.12	33.80	15.62	14.99	9.13	29.58	14.46	12.19	9.11
Claude-3.5-Sonnet	30.99	14.23	15.59	9.38	30.28	12.43	15.25	9.27	30.63	16.04	16.26	9.35

($\epsilon \geq 8$), our attacks have higher PRECISION and RECALL, indicating that our approach can attack the DP text sanitization approach under a practical privacy budget. In contrast, for a smaller privacy budget, both PRECISION and RECALL are low, indicating that only a minimal amount of sensitive information can be recovered.

VI. RELATED WORK

This section mainly introduces related works with ours in LLMs’s security and privacy. Here, we category them into the following several perspectives, i.e., Training data leakage in LLMs, Training data memorization in LLMs, Prompt leakage in LLMs and Membership inference attacks for LLMs.

Training data leakage in LLMs. The state-of-the-art LLMs are often trained on web crawl data, which may include personal data. Extensive studies target stealing sensitive information from the training data of LLMs. Huang et al. [30]

query the email address and owner names in pre-trained LLMs and demonstrate pre-trained LLMs leakage PII due to memorization. Lukas et al. [38] introduce game-based definitions for PII leakage and evaluate attacks on GPT-2. They demonstrate that data scrubbing can not entirely prevent the leakage of PII, but DP training can substantially mitigate the risk of PII leakage. Kim et al. [34] propose a framework for data subjects to measure their level of PII leakage in LLMs. Liu et al. [37] present PreCurious, where attackers can extract fine-tuning data by releasing pre-trained LLMs.

Training data memorization in LLMs. A line of work on extracting training data from LLMs reveals that LLMs can memorize and regenerate the training data. Inan et al. [33] investigate how to quantify the user content leakage in LLMs and demonstrate that LLMs memorize training data. Carlini et al. [19] extract hundreds of verbatim text from the training data

TABLE XII
RESULTS OF THE WHITE-BOX FINE-TUNING-BASED ATTACKS AGAINST THE WORD-LEVEL DP ON PILE-CC.

Models	$\epsilon = 12$			$\epsilon = 8$			$\epsilon = 4$		
	SUCC	RECALL	PREC	SUCC	RECALL	PREC	SUCC	RECALL	PREC
OPT-350M	14.60	4.47	4.30	8.60	2.01	2.59	0.90	0.27	0.24
OPT-1.3B	35.90	13.21	15.46	18.80	4.78	5.34	0.80	0.14	0.10
OPT-6.7B	36.10	14.19	16.46	21.90	5.85	7.29	2.40	0.59	0.80
GPT-Neo-1.3B	13.80	4.30	3.96	10.00	2.42	2.63	1.80	0.46	0.66
GPT-Neo-2.7B	18.30	5.63	5.30	12.40	2.88	3.27	2.60	0.77	1.00
GPT-J-6B	19.70	6.08	5.75	14.50	3.53	3.98	1.70	0.50	0.38
Pythia-1.4B	31.70	10.85	12.38	15.10	3.42	4.71	1.80	0.38	0.41
Pythia-2.8B	33.80	12.22	14.39	14.60	3.37	4.18	2.00	0.45	0.48
Pythia-6.9B	49.40	12.46	13.90	19.20	4.96	5.65	2.00	0.44	0.77

TABLE XIII
RESULTS OF THE WHITE-BOX FINE-TUNING-BASED ATTACKS AGAINST THE WORD-LEVEL DP ON PILE-WIKI.

Models	$\epsilon = 12$			$\epsilon = 8$			$\epsilon = 4$		
	SUCC	RECALL	PREC	SUCC	RECALL	PREC	SUCC	RECALL	PREC
OPT-350M	24.00	4.87	4.44	21.10	3.12	3.82	9.80	1.14	1.23
OPT-1.3B	60.90	17.95	19.88	48.50	8.81	9.91	9.80	1.11	1.20
OPT-6.7B	63.80	19.45	22.34	51.80	9.95	11.82	8.90	0.89	1.09
GPT-Neo-1.3B	32.50	7.18	6.15	21.50	2.91	3.03	7.80	0.85	0.98
GPT-Neo-2.7B	28.30	5.93	5.20	23.30	3.28	3.70	8.20	0.82	1.05
GPT-J-6B	45.20	11.03	10.92	34.00	5.28	5.86	6.50	0.68	0.74
Pythia-1.4B	51.20	12.62	14.10	35.90	5.55	6.74	6.00	0.67	1.00
Pythia-2.8B	49.90	12.71	14.09	40.20	6.34	7.89	6.90	0.74	0.84
Pythia-6.9B	49.40	12.46	13.90	34.50	5.37	6.52	5.50	0.60	0.72

TABLE XIV
RESULTS OF THE WHITE-BOX FINE-TUNING-BASED ATTACKS AGAINST THE WORD-LEVEL DP ON PILE-ENRON.

Models	$\epsilon = 12$			$\epsilon = 8$			$\epsilon = 4$		
	SUCC	RECALL	PREC	SUCC	RECALL	PREC	SUCC	RECALL	PREC
OPT-350M	29.50	6.43	7.45	20.90	3.08	3.89	9.30	1.19	2.66
OPT-1.3B	56.70	15.63	19.69	34.60	5.89	8.52	10.90	1.26	1.82
OPT-6.7B	58.30	16.99	20.99	38.60	7.22	9.43	5.20	0.58	0.95
GPT-Neo-1.3B	31.80	6.45	7.27	16.90	2.29	3.01	8.80	1.21	1.61
GPT-Neo-2.7B	33.70	7.59	8.65	18.60	2.80	3.70	8.30	1.04	1.66
GPT-J-6B	39.90	9.69	11.20	20.30	3.32	3.99	4.20	0.51	0.93
Pythia-1.4B	46.40	11.91	14.70	26.40	4.12	5.80	4.90	0.58	1.80
Pythia-2.8B	50.00	13.15	15.94	21.50	3.35	4.82	3.30	0.35	0.85
Pythia-6.9B	56.30	16.37	20.46	30.80	5.89	7.85	4.20	0.69	1.36

of GPT-2, including personal information (e.g., names, email addresses), indicating that an adversary can recover personal data from LMs through querying. Nasr et al. [45] further investigate the extraction of training data on extensive LLMs and introduce a divergence attack for aligned ChatGPT to recover more data. Carlini et al. [18] propose a new definition for quantifying the upper bounds of LLMs memorization. Kim et al. [34] presents a framework to prob PII leakage for data subjects to evaluate the level of privacy leakage in LLMs. Patil et al. [48] demonstrate that deleting sensitive information from LLMs for even the state-of-the-art model editing methods (e.g., ROME [43]) is difficult.

Prompt leakage in LLMs. In LLMs, the prompt is commonly used to control the text generated by LLMs, and the prompt leakage has recently raised privacy concerns because an adversary can perform prompt extraction attacks to recover the original prompt. For example, Zhang et al. [64] perform a text-based attack that can effectively recover prompts. Sha et al. [51] propose a method that classifies prompts and reconstructs them based on the generated text of LLMs. Agarawal et al. [8] investigate the prompt leakage in retrieval-augmented generation (RAG) system. Hui et al. [31] design a prompt extraction attack framework named PLeak based on gradient-based optimization.

TABLE XV
EXAMPLE OF THE WHITE-BOX FINE-TUNING ATTACKS AGAINST THE WORD-LEVEL DP ON PILE-CC AND PILE-ENRON.

	Pile-CC	Pile-Enron
Original	<p>The Foreign Intelligence Surveillance Court has never had a heavier workload nor played a more important role as arbiter of the scope of government surveillance than it does today. But little information about the Court, which was established by the Foreign Intelligence Surveillance Act (FISA) of 1978, has been readily available in the public domain – not even a complete list of its members.</p>	<p>Will do. Steven J Kean 05/11/2001 08:35 AM To: Jeff Dasovich/NA/Enron cc: Sandra McCubbin/NA/Enron@Enron, Paul Kaufman/Enron@EnronXGate, James D Steffes/NA/Enron@Enron, Richard Shapiro/NA/Enron@Enron, Susan J Mara/NA/Enron@ENRON Subject: Ken Lay spoke with several California CEOs this morning and urged them to get personally involved in pushing for a comprehensive set of reforms. Three expressed willingness to help. Scott McNealy (Sun): contact person - Piper Cole (piper.cole@sun.com); scott.mcnealy@engeng.sun.com.</p>
DP-sanitized (Madlib, $\epsilon = 8$)	<p>movement exchange intelligence surveillance court whose... immediately a heavier shorten justice picked bottom too important conventions longer arbiter of started indicate capital administration surveillance amount but depends borrowed: turning little identifying tom position take; has prior 1959 removal has lavrov intelligence surveillance act (fisa) to debated say beckham being centrifuges available after the behalf sanctum – what even s complete instance related of attended spring</p>	<p>adjustments do united steven norwich mallard answering given: jeff districtincumbent enron cc: sandra @ enron recently michael akha _ cecil d gha aig fly mueller haplogroup enron detrick susan emāmzādeh @ enron writings applies ken arms talked alive several california worried official midday working urged actually laid get personally posed where pushes complaints burns comprehensive world of reforms see three convinced undermine begun help normally browne mcnealy (sun (s contact family – piper armstrong or u2019ll) 2 @ either</p>
Reconstructed (Pythia-1.3B)	<p>[FISA] The Intelligence Surveillance Court is an independent, non-partisan body that arbitrates disputes between the government and private parties regarding the use of electronic surveillance. But it also plays a role in determining whether or not FISA warrants are valid under current law. The FISC was created by Congress to.</p>	<p>===== From: Steven Leppert@ENRON on 03/01/2001 09:00 AM To: Jeff Dasovich/NA/Enron@Enron, Michael Etringer/HOU/ECT@ECT, Susan J Mara/NA/Enron@ENRON, Sandra McCubbin/NA/Enron@Enron, Paul Kaufman/PDX/ECT@ECT, Mary H</p>
Reconstructed (Pythia-2.8B)	<p>The Foreign Intelligence Surveillance Court,... It is not clear how long this body will remain in charge of approving and authorizing national security wiretaps. But it does have some authority to make that decision on its own under the FISA Amendments Act (FAA), which says</p>	<p>The EnronOnline Team is meeting with Jeff Skilling today. 8 From: Steven J Kean@EES on 05/01/2001 09:47 AM To: Michael McDonald/LON/ECT@ECT, David Port/Market Risk/Corp/Enron@ENRON, Susan Skarness/HOU/ECT@ECT, Mark Schroeder/LON/ECT</p>
Reconstructed (Pythia-6.9B)	<p>The FISA Court is not a rubber stamp for any Administration request. It is an independent arbiter of whether or not the government's surveillance activities are in compliance with the law, and it was created by Congress under the Foreign Intelligence Surveillance Act (FISA). So let me get this straight – we have</p>	<p>We have Steven J Kean@EES, Jeff Dasovich/NA/Enron on the phone. Jeff D'Alessandro@ECT 10/25/2000 06:29 AM To: Sandra McCubbin/SFO/EES@EES cc: Richard Shapiro/HOU/EES@EES, James D Steffes/HOU/EES@</p>
Reconstructed (OPT-6.7B)	<p>The Foreign Intelligence Surveillance Court is... A more independent and less politicized judge than the FISA Court. It's an administrative body that approves all government surveillance requests, but it doesn't have to follow the same rules as the FISA Act. The Foreign Intelligence Surveillance Act (FISA) was passed in 1978 after the Church Committee</p>	<p>----- From: Steven J Kean/ENRON@enronXgate on 04/18/2001 09:33 AM To: Jeff Dasovich/NA/Enron@Enron cc: Sandra McCubbin/NA/Enron@Enron, Michael Tribolet/ENRON@enronxgate, Richard Shapiro/HOU/EES@EES, Susan</p>
Reconstructed (GPT-J-6B)	<p>Â Section 218 FISA The PATRIOT Act expanded the reach of executive branch authority under which it could issue orders directing telecommunications providers to turn over bulk records. But for all that, Congress passed another piece in December 2005 – called the National Security Agency's Intelligence Surveillance Activities Act or "Smith Verizon Orders After the fact</p>	<p>David Boies 325 E. 57th Street 35, New York NY 10021 david@boiesandnobolsky.com For Sara and Steve Williams Jeff Dasovich/NA/Enron@ENRON 08/11/2001 07:41 AM To: Joseph Alamo/NA/Enron@Enron cc: Sandra McCubbin/NA/Enron@En</p>

Membership inference attacks for LLMs. Compared to training data extraction attacks, membership inference attacks (MIAs) aim to determine whether a provided text is in the training dataset for given LLMs. For instance, Mireshghallah et al. [44] present a membership inference attack based on likelihood ratio hypothesis testing for Masked LLMs. Mattern et al. [40] propose an attack based on the loss value of neighborhood for LLMs. Shi et al. [52] detect pre-training data on LLMs without access to the pre-training dataset and demonstrate that currently, GPT-3 may be trained on copyrighted content.

Comparison with existing studies. Existing works discovered the "current" privacy concerns, which could be addresses by DP, the de facto privacy standard. However, our work, focusing on "future" privacy concerns as motivated in Sec. I,

demonstrates that DP might have the potential vulnerability in the era of LLMs, which can recover the privacy from the DP-sanitized text.

VII. MITIGATION & DISCUSSION

This section gives potential mitigation strategies to further preserve privacy against the privacy leakage discovered in this paper. We also discussed the technical limitation of this paper. The ethics statement is attached in Appx. VIII-D.

Mitigation via machine unlearning in LLMs. Machine unlearning [46] is a technology of removing specific data or learned knowledge from a model. In particular, the pre-training data of LLMs includes a large amount of copyrighted content [21]. Several works [23], [62] investigate leveraging machine unlearning technology to forget the copyrighted content in LLMs. Similarly, our reconstruction attacks can be

TABLE XVI
RESULTS OF THE WHITE-BOX FINE-TUNING-BASED ATTACKS AGAINST THE WORD-LEVEL DP ON WIKIMIA.

Models	$\epsilon = 12$			$\epsilon = 8$			$\epsilon = 4$		
	SUCC	RECALL	PREC	SUCC	RECALL	PREC	SUCC	RECALL	PREC
OPT-350M	34.88	6.77	6.65	24.42	3.37	4.46	11.24	1.15	1.68
OPT-1.3B	60.47	15.88	17.68	43.80	7.93	8.65	6.98	0.68	0.77
OPT-6.7B	63.57	17.52	18.09	45.35	8.49	9.36	4.26	0.47	0.45
GPT-Neo-1.3B	27.13	4.68	4.38	19.77	2.44	2.81	5.04	0.42	0.65
GPT-Neo-2.7B	35.27	7.31	6.28	21.71	3.12	3.18	6.20	0.62	0.78
GPT-J-6B	43.02	9.92	8.67	31.78	5.16	5.34	5.04	0.48	0.71
Pythia-1.4B	39.92	9.56	9.76	32.17	5.09	6.60	4.65	0.43	0.63
Pythia-2.8B	50.00	12.28	13.20	35.27	5.16	6.36	4.26	0.48	0.92
Pythia-6.9B	46.51	11.28	11.00	30.62	4.70	5.40	3.49	0.34	0.43

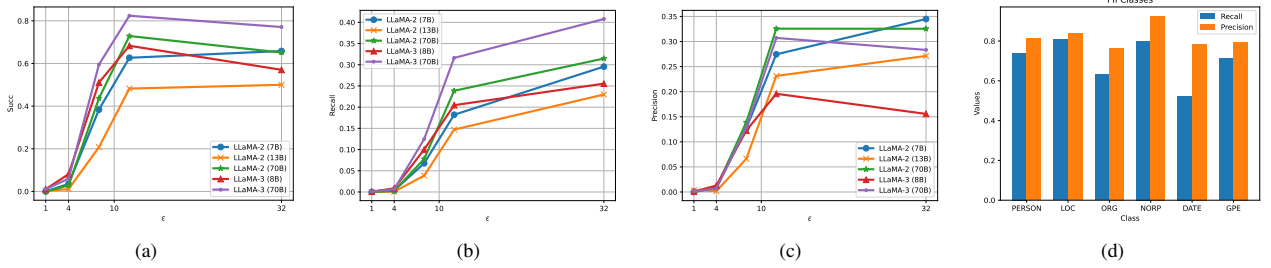


Fig. 3. Fig. 3(a), Fig. 3(b) and Fig. 3(c) provide the correlation between the SUCC, RECALL, PRECISION and privacy budgets, respectively. Fig. 3(d) shows the PRECISION and RECALL for different PII classes on WikiMIA using word-level DP under $\epsilon = 8$.

mitigated if we can leverage machine unlearning to eliminate the memory of sensitive information in pre-training data. Nevertheless, Shi et al. [52] state that the model trained to forget copyrighted content by machine unlearning can still output related content using the specific query. Future work may explore the potential of using machine unlearning to mitigate our reconstruction attacks.

Mitigation via cryptography. Cryptography could potentially address the issues outlined in this paper, as the mapping space between plaintext and ciphertext in cryptographic algorithms is sufficiently complex to prevent reconstruction attacks similar to those discussed here. However, considering the time and space complexity inherent in both cryptographic algorithms and training large language models, deploying cryptography for LLM applications may not be feasible.

PII classes. We also conducted experiments to show the performance of our attacks for different PII classes, which have different degrees of sensitive information leakage. Direct identifiers (e.g., names) leak more sensitive information than quasi-identifiers (e.g., addresses). For experimental settings, we select six classes (e.g., person, address, organization), and apply the black-box instruction-based attack to ChatGPT-4 with the word-level DP under privacy budget $\epsilon = 8.0$. Fig. 3(d) in Sec. V-H shows the PRECISION and RECALL for different PII classes on WikiMIA. The results demonstrate that our reconstruction attacks exhibit varying levels of effectiveness in recovering different types of sensitive information.

Limitation. In this study, we could not conduct useful ablation studies to determine whether the training data played

a crucial role in LLMs’ ability to recover privacy. On one hand, performing such ablation studies on black-box attacks is infeasible due to the unpublished training data of the LLMs, despite their promising recovery rates. On the other hand, for LLMs with specified training data, we tested white-box attacks using DP-sanitized text, where the corresponding original text was not included in the LLMs’ training data. Specifically, we prompted the same fine-tuned LLMs as those in Tab. XIII using DP-sanitized text from WikiMIA (which was guaranteed not to have been seen by the LLMs). The results, shown in Tab. XVI in Sec. V-H, indicate similar recovery rates to those in Tab. XIII. However, these similar results further confirm that white-box LLMs trained on a limited number of text data do not exhibit sufficient capability to perform our attacks.

VIII. CONCLUSION

This paper identifies a potential privacy risk associated with applying DP in LLMs. We demonstrate that it is possible to reconstruct the text sanitized by the DP through querying LLMs. Based on the access to trained LLMs, we propose black-box instruction-based attacks and white-box fine-tuning-based attacks. Extensive experimental results show that our attacks effectively reconstruct the DP-sanitized text under a practical privacy budget (e.g., $\epsilon \geq 8$) against both word-level and sentence-level DP.

REFERENCES

- [1] Anthropic api. <https://api.anthropic.com/v1>.
- [2] English ner in flair. <https://huggingface.co/flair/ner-english-ontonotes-large>.

- [3] llama 13b is performing worse than llama 7b? https://www.reddit.com/r/LocalLLaMA/comments/15cyzyw/llama_13b_is_performing_worse_than_llama_7b/.
- [4] Openai api. <https://api.openai.com/v1>.
- [5] The pile. <https://pile.eleuther.ai/>.
- [6] Pile. uncopyrighted. <https://huggingface.co/datasets/monology/pile-uncopyrighted>.
- [7] Josh Achiam, Steven Adler, Sandhini Agarwal, Lama Ahmad, Ilge Akkaya, Florencia Leoni Aleman, Diogo Almeida, Janko Altschmidt, Sam Altman, Shyamal Anadkat, et al. Gpt-4 technical report. *arXiv preprint arXiv:2303.08774*, 2023.
- [8] Divyansh Agarwal, Alexander R Fabbri, Philippe Laban, Shafiq Joty, Caiming Xiong, and Chien-Sheng Wu. Investigating the prompt leakage effect and black-box defenses for multi-turn llm interactions. *arXiv preprint arXiv:2404.16251*, 2024.
- [9] AI@Meta. Llama 3 model card, 2024.
- [10] Alan Akbik, Tanja Bergmann, Duncan Blythe, Kashif Rasul, Stefan Schweter, and Roland Vollgraf. FLAIR: An easy-to-use framework for state-of-the-art NLP. In Waleed Ammar, Annie Louis, and Nasrin Mostafazadeh, editors, *Proceedings of the 2019 Conference of the North American Chapter of the Association for Computational Linguistics (Demonstrations)*, pages 54–59, Minneapolis, Minnesota, June 2019. Association for Computational Linguistics.
- [11] Anthropic. Claude. <https://www.anthropic.com/>.
- [12] Apple. Differential privacy overview. https://www.apple.com/privacy/docs/Differential_Privacy_Overview.pdf, 2022.
- [13] Stella Biderman, Hailey Schoelkopf, Quentin Gregory Anthony, Herbie Bradley, Kyle O’Brien, Eric Hallahan, Mohammad Aflah Khan, Shivanishu Purohit, USVSN Sai Prashanth, Edward Raff, et al. Pythia: A suite for analyzing large language models across training and scaling. In *International Conference on Machine Learning*, pages 2397–2430. PMLR, 2023.
- [14] Steven Bird, Ewan Klein, and Edward Loper. *Natural language processing with Python: analyzing text with the natural language toolkit*. O’Reilly Media, Inc., 2009.
- [15] Sid Black, Gao Leo, Phil Wang, Connor Leahy, and Stella Biderman. GPT-Neo: Large Scale Autoregressive Language Modeling with Mesh-Tensorflow, March 2021. If you use this software, please cite it using these metadata.
- [16] Tom Brown, Benjamin Mann, Nick Ryder, Melanie Subbiah, Jared D Kaplan, Prafulla Dhariwal, Arvind Neelakantan, Pranav Shyam, Girish Sastry, Amanda Askell, Sandhini Agarwal, Ariel Herbert-Voss, Gretchen Krueger, Tom Henighan, Rewon Child, Aditya Ramesh, Daniel Ziegler, Jeffrey Wu, Clemens Winter, Chris Hesse, Mark Chen, Eric Sigler, Mateusz Litwin, Scott Gray, Benjamin Chess, Jack Clark, Christopher Berner, Sam McCandlish, Alec Radford, Ilya Sutskever, and Dario Amodei. Language models are few-shot learners. In H. Larochelle, M. Ranzato, R. Hadsell, M.F. Balcan, and H. Lin, editors, *Advances in Neural Information Processing Systems*, volume 33, pages 1877–1901. Curran Associates, Inc., 2020.
- [17] U.S. Census Bureau. Census bureau sets key parameters to protect privacy in 2020 census results. <https://web.archive.org/web/20240408192318/https://www.census.gov/newsroom/press-releases/2021/2020-census-key-parameters.html>. Accessed: 2024-07-10.
- [18] Nicholas Carlini, Daphne Ippolito, Matthew Jagielski, Katherine Lee, Florian Tramèr, and Chiyuan Zhang. Quantifying memorization across neural language models. In *The Eleventh International Conference on Learning Representations*, 2023.
- [19] Nicholas Carlini, Florian Tramèr, Eric Wallace, Matthew Jagielski, Ariel Herbert-Voss, Katherine Lee, Adam Roberts, Tom Brown, Dawn Song, Ulfar Erlingsson, Alina Oprea, and Colin Raffel. Extracting training data from large language models. In *30th USENIX Security Symposium (USENIX Security 21)*, pages 2633–2650. USENIX Association, August 2021.
- [20] Ricardo Silva Carvalho, Theodore Vasiloudis, Oluwaseyi Feyisetan, and Ke Wang. Tem: High utility metric differential privacy on text. In *Proceedings of the 2023 SIAM International Conference on Data Mining (SDM)*, pages 883–890. SIAM, 2023.
- [21] Kent Chang, Mackenzie Cramer, Sandeep Soni, and David Bamman. Speak, memory: An archaeology of books known to ChatGPT/GPT-4. In Houda Bouamor, Juan Pino, and Kalika Bali, editors, *Proceedings of the 2023 Conference on Empirical Methods in Natural Language Processing*, pages 7312–7327, Singapore, December 2023. Association for Computational Linguistics.
- [22] Cynthia Dwork, Frank McSherry, Kobbi Nissim, and Adam Smith. Calibrating noise to sensitivity in private data analysis. In Shai Halevi and Tal Rabin, editors, *Theory of Cryptography*, pages 265–284, Berlin, Heidelberg, 2006. Springer Berlin Heidelberg.
- [23] Ronen Eldan and Mark Russinovich. Who’s harry potter? approximate unlearning in llms. *arXiv preprint arXiv:2310.02238*, 2023.
- [24] Oluwaseyi Feyisetan, Borja Balle, Thomas Drake, and Tom Diethe. Privacy- and utility-preserving textual analysis via calibrated multivariate perturbations. In *Proceedings of the 13th International Conference on Web Search and Data Mining, WSDM ’20*, page 178–186, New York, NY, USA, 2020. Association for Computing Machinery.
- [25] Oluwaseyi Feyisetan, Tom Diethe, and Thomas Drake. Leveraging hierarchical representations for preserving privacy and utility in text. In *2019 IEEE International Conference on Data Mining (ICDM)*, pages 210–219, 2019.
- [26] Leo Gao, Stella Biderman, Sid Black, Laurence Golding, Travis Hoppe, Charles Foster, Jason Phang, Horace He, Anish Thite, Noa Nabeshima, et al. The pile: An 800gb dataset of diverse text for language modeling. *arXiv preprint arXiv:2101.00027*, 2020.
- [27] GDPR.EU. Everything you need to know about the “right to be forgotten”. <https://gdpr.eu/right-to-be-forgotten/?cn-reloaded=1>. Accessed: 2024-07-11.
- [28] Matthew Honnibal, Ines Montani, Sofie Van Landeghem, and Adriane Boyd. spaCy: Industrial-strength Natural Language Processing in Python, 2020.
- [29] Edward J Hu, Yelong Shen, Phillip Wallis, Zeyuan Allen-Zhu, Yuanzhi Li, Shean Wang, Lu Wang, and Weizhu Chen. Lora: Low-rank adaptation of large language models. *arXiv preprint arXiv:2106.09685*, 2021.
- [30] Jie Huang, Hanyin Shao, and Kevin Chen-Chuan Chang. Are large pre-trained language models leaking your personal information? In Yoav Goldberg, Zornitsa Kozareva, and Yue Zhang, editors, *Findings of the Association for Computational Linguistics: EMNLP 2022*, pages 2038–2047, Abu Dhabi, United Arab Emirates, December 2022. Association for Computational Linguistics.
- [31] Bo Hui, Haolin Yuan, Neil Gong, Philippe Burlina, and Yinzhi Cao. Pleak: Prompt leaking attacks against large language model applications. *arXiv preprint arXiv:2405.06823*, 2024.
- [32] Timour Igamberdiev and Ivan Habernal. DP-BART for privatized text rewriting under local differential privacy. In Anna Rogers, Jordan Boyd-Graber, and Naoaki Okazaki, editors, *Findings of the Association for Computational Linguistics: ACL 2023*, pages 13914–13934, Toronto, Canada, July 2023. Association for Computational Linguistics.
- [33] Huseyin A Inan, Osman Ramadan, Lukas Wutschitz, Daniel Jones, Victor Rühle, James Withers, and Robert Sim. Training data leakage analysis in language models. *arXiv preprint arXiv:2101.05405*, 2021.
- [34] Siwon Kim, Sangdoo Yun, Hwaran Lee, Martin Gubri, Sungroh Yoon, and Seong Joon Oh. Propile: Probing privacy leakage in large language models. In A. Oh, T. Naumann, A. Globerson, K. Saenko, M. Hardt, and S. Levine, editors, *Advances in Neural Information Processing Systems*, volume 36, pages 20750–20762. Curran Associates, Inc., 2023.
- [35] Bryan Klimt and Yiming Yang. The enron corpus: A new dataset for email classification research. In Jean-François Boulicaut, Floriana Esposito, Fosca Giannotti, and Dino Pedreschi, editors, *Machine Learning: ECML 2004*, pages 217–226, Berlin, Heidelberg, 2004. Springer Berlin Heidelberg.
- [36] Satyapriya Krishna, Rahul Gupta, and Christophe Dupuy. ADePT: Auto-encoder based differentially private text transformation. In Paola Merlo, Jörg Tiedemann, and Reut Tsarfay, editors, *Proceedings of the 16th Conference of the European Chapter of the Association for Computational Linguistics: Main Volume*, pages 2435–2439, Online, April 2021. Association for Computational Linguistics.
- [37] Ruixuan Liu, Tianhao Wang, Yang Cao, and Li Xiong. Precurious: How innocent pre-trained language models turn into privacy traps. *arXiv preprint arXiv:2403.09562*, 2024.
- [38] Nils Lukas, Ahmed Salem, Robert Sim, Shruti Tople, Lukas Wutschitz, and Santiago Zanella-Béguelin. Analyzing leakage of personally identifiable information in language models. In *2023 IEEE Symposium on Security and Privacy (SP)*, pages 346–363, 2023.
- [39] Sourab Mangrulkar, Sylvain Gugger, Lysandre Debut, Younes Belkada, Sayak Paul, and Benjamin Bossan. Peft: State-of-the-art parameter-efficient fine-tuning methods. <https://github.com/huggingface/peft>, 2022.
- [40] Justus Mattern, Fatemehsadat Miresghallah, Zhijing Jin, Bernhard Schoelkopf, Mrinmaya Sachan, and Taylor Berg-Kirkpatrick. Mem-

bership inference attacks against language models via neighbourhood comparison. In Anna Rogers, Jordan Boyd-Graber, and Naoaki Okazaki, editors, *Findings of the Association for Computational Linguistics: ACL 2023*, pages 11330–11343, Toronto, Canada, July 2023. Association for Computational Linguistics.

[41] Justus Mattern, Benjamin Weggenmann, and Florian Kerschbaum. The limits of word level differential privacy. In Marine Carpuat, Marie-Catherine de Marneffe, and Ivan Vladimir Meza Ruiz, editors, *Findings of the Association for Computational Linguistics: NAACL 2022*, pages 867–881, Seattle, United States, July 2022. Association for Computational Linguistics.

[42] Frank McSherry and Kunal Talwar. Mechanism design via differential privacy. In *48th Annual IEEE Symposium on Foundations of Computer Science (FOCS'07)*, pages 94–103, 2007.

[43] Kevin Meng, David Bau, Alex J Andonian, and Yonatan Belinkov. Locating and editing factual associations in GPT. In Alice H. Oh, Alekh Agarwal, Danielle Belgrave, and Kyunghyun Cho, editors, *Advances in Neural Information Processing Systems*, 2022.

[44] Fatemehsadat Miresghallah, Kartik Goyal, Archit Niyal, Taylor Berg-Kirkpatrick, and Reza Shokri. Quantifying privacy risks of masked language models using membership inference attacks. In Yoav Goldberg, Zornitsa Kozareva, and Yue Zhang, editors, *Proceedings of the 2022 Conference on Empirical Methods in Natural Language Processing*, pages 8332–8347, Abu Dhabi, United Arab Emirates, December 2022. Association for Computational Linguistics.

[45] Milad Nasr, Nicholas Carlini, Jonathan Hayase, Matthew Jagielski, A. Feder Cooper, Daphne Ippolito, Christopher A. Choquette-Choo, Eric Wallace, Florian Tramèr, and Katherine Lee. Scalable extraction of training data from (production) language models, 2023.

[46] Thanh Tam Nguyen, Thanh Trung Huynh, Phi Le Nguyen, Alan Wee-Chung Liew, Hongzhi Yin, and Quoc Viet Hung Nguyen. A survey of machine unlearning. *arXiv preprint arXiv:2209.02299*, 2022.

[47] Adam Paszke, Sam Gross, Francisco Massa, Adam Lerer, James Bradbury, Gregory Chanan, Trevor Killeen, Zeming Lin, Natalia Gimelshein, Luca Antiga, et al. Pytorch: An imperative style, high-performance deep learning library. *Advances in neural information processing systems*, 32, 2019.

[48] Vaidehi Patil, Peter Hase, and Mohit Bansal. Can sensitive information be deleted from LLMs? objectives for defending against extraction attacks. In *The Twelfth International Conference on Learning Representations*, 2024.

[49] Jeffrey Pennington, Richard Socher, and Christopher Manning. GloVe: Global vectors for word representation. In Alessandro Moschitti, Bo Pang, and Walter Daelemans, editors, *Proceedings of the 2014 Conference on Empirical Methods in Natural Language Processing (EMNLP)*, pages 1532–1543, Doha, Qatar, October 2014. Association for Computational Linguistics.

[50] Ildikó Pilán, Pierre Lison, Lilja Øvrelid, Anthi Papadopoulou, David Sánchez, and Montserrat Batet. The text anonymization benchmark (tab): A dedicated corpus and evaluation framework for text anonymization. *Computational Linguistics*, 48(4):1053–1101, 2022.

[51] Zeyang Sha and Yang Zhang. Prompt stealing attacks against large language models. *arXiv preprint arXiv:2402.12959*, 2024.

[52] Weijia Shi, Anirudh Ajith, Mengzhou Xia, Yangsibo Huang, Daogao Liu, Terra Blevins, Danqi Chen, and Luke Zettlemoyer. Detecting pre-training data from large language models. In *The Twelfth International Conference on Learning Representations*, 2024.

[53] Gemma Team. Gemma, 2024.

[54] Hugo Touvron, Thibaut Lavril, Gautier Izacard, Xavier Martinet, Marie-Anne Lachaux, Timothée Lacroix, Baptiste Rozière, Naman Goyal, Eric Hambro, Faisal Azhar, et al. Llama: Open and efficient foundation language models. *arXiv preprint arXiv:2302.13971*, 2023.

[55] Hugo Touvron, Louis Martin, Kevin Stone, Peter Albert, Amjad Almahairi, Yasmine Babaei, Nikolay Bashlykov, Soumya Batra, Prajwal Bhargava, Shrutli Bhosale, et al. Llama 2: Open foundation and finetuned chat models. *arXiv preprint arXiv:2307.09288*, 2023.

[56] Saiteja Utpala, Sara Hooker, and Pin Yu Chen. Dp-prompt github repository. https://github.com/SaitejaUtpala/dp_prompt.

[57] Saiteja Utpala, Sara Hooker, and Pin-Yu Chen. Locally differentially private document generation using zero shot prompting. In Houda Bouamor, Juan Pino, and Kalika Bali, editors, *Findings of the Association for Computational Linguistics: EMNLP 2023*, pages 8442–8457, Singapore, December 2023. Association for Computational Linguistics.

[58] Ashish Vaswani, Noam Shazeer, Niki Parmar, Jakob Uszkoreit, Llion Jones, Aidan N Gomez, Łukasz Kaiser, and Illia Polosukhin. Attention is all you need. In I. Guyon, U. Von Luxburg, S. Bengio, H. Wallach, R. Fergus, S. Vishwanathan, and R. Garnett, editors, *Advances in Neural Information Processing Systems*, volume 30. Curran Associates, Inc., 2017.

[59] Ben Wang and Aran Komatsuzaki. GPT-J-6B: A 6 Billion Parameter Autoregressive Language Model. <https://github.com/kingoflolz/mesh-transformer-jax>, May 2021.

[60] Sam Witteveen and Martin Andrews. Paraphrasing with large language models. In Alexandra Birch, Andrew Finch, Hiroaki Hayashi, Ioannis Konstas, Thang Luong, Graham Neubig, Yusuke Oda, and Katsuhito Sudoh, editors, *Proceedings of the 3rd Workshop on Neural Generation and Translation*, pages 215–220, Hong Kong, November 2019. Association for Computational Linguistics.

[61] Thomas Wolf, Lysandre Debut, Victor Sanh, Julien Chaumond, Clement Delangue, Anthony Moi, Pierric Cistac, Tim Rault, Remi Louf, Morgan Funtowicz, Joe Davison, Sam Shleifer, Patrick von Platen, Clara Ma, Yacine Jernite, Julien Plu, Canwen Xu, Teven Le Scao, Sylvain Gugger, Mariama Drame, Quentin Lhoest, and Alexander Rush. Transformers: State-of-the-art natural language processing. In Qun Liu and David Schlangen, editors, *Proceedings of the 2020 Conference on Empirical Methods in Natural Language Processing: System Demonstrations*, pages 38–45, Online, October 2020. Association for Computational Linguistics.

[62] Dawen Zhang, Pamela Finckenberg-Broman, Thong Hoang, Shidong Pan, Zhenchang Xing, Mark Staples, and Xiwei Xu. Right to be forgotten in the era of large language models: Implications, challenges, and solutions. *arXiv preprint arXiv:2307.03941*, 2023.

[63] Susan Zhang, Stephen Roller, Naman Goyal, Mikel Artetxe, Moya Chen, Shuohui Chen, Christopher Dewan, Mona Diab, Xian Li, Xi Victoria Lin, et al. Opt: Open pre-trained transformer language models. *arXiv preprint arXiv:2205.01068*, 2022.

[64] Yiming Zhang, Nicholas Carlini, and Daphne Ippolito. Effective prompt extraction from language models, 2024.

APPENDIX

A. Language Models

Given a sequence $\mathbf{x} = \{x_1, x_2, \dots, x_n\}$ with n tokens from the vocabulary \mathcal{V} , an autoregressive language model (LM) is trained to predict the next token by modeling the conditional probability distribution $\Pr(x_i | x_1, x_2, \dots, x_{i-1}; \theta)$ over the sequence of previous tokens, where $i = \{1, 2, \dots, n\}$. We denote the probability distribution of an autoregressive LM with parameters θ over the sequence \mathbf{x} as:

$$\Pr(\mathbf{x}; \theta) = \prod_{i=1}^n \Pr(x_i | x_1, x_2, \dots, x_{i-1}; \theta). \quad (5)$$

At the training stage, the objective of the standard language modeling is to minimize the negative log-likelihood as $\mathcal{L}(\theta) = -\sum_{i=0}^n \log \Pr(x_i | x_1, x_2, \dots, x_{i-1}; \theta)$, where the model outputs the probability distribution of all possible tokens, and calculate the logarithm of probability for calculating the loss function. In the inference stage, the autoregressive LM is prompted by a prefix to generate a new text. Specifically, LMs iteratively output each token x'_i by sampling from the conditional probability distribution over the sequence of all previously generated tokens and prefixes. We denote this procedure as $\mathbf{x}' = \text{GENERATE}(\mathbf{y}, \theta)$, where \mathbf{x}' is generated text and \mathbf{y} is given prefix.

Our work focuses on the state-of-the-art large language models (LLMs), which are usually based on the Transformer [58] architecture with billions of parameters (e.g., GPT-3 [7], Llama 2 [55]). Generally, there are three training phases

for LLMs: pre-training, supervised learning, and reinforcement learning from human feedback (RLHF). In the pre-training phase, the LLM is trained to predict the next token for the given prefix from the public large-scale raw text crawled on the Internet. We refer to the dataset used in the pre-training stage as the pre-training dataset. During the supervised learning phase, the LLM is fine-tuned to follow the instructions from the prompt and response. Then, in the reinforcement learning phase, the LLM is optimized by a reward model, which is trained using the feedback for model response from humans. Note that the overall quality of response of LLM can be improved via supervised learning and RLHF. We refer to the model after the pre-trained stage as the pre-trained LLM and the model after the supervised learning and reinforcement learning stages as the instruction-tuned LLM.

B. Word- and Sentence-level DP Approaches

Word-level DP approaches. The goal of the word-level DP is to perturb each word in a sentence under the metric DP. Formally, consider a sequence $\mathbf{x} = \{x_1, x_2, \dots, x_n\}$ with n tokens, each token x_i is converted to a m -dimensional word embedding $\phi_i = \phi(x_i)$ by a pre-trained word embedding model $\phi: \mathcal{V} \rightarrow \mathbb{R}^m$, where \mathcal{V} represents the vocabulary. To obtain the noisy embedding $\tilde{\phi}_i$, a noise \mathbf{z} sampled from a multivariate probability distribution $p_e(\mathbf{z})$ is injected into ϕ_i . Subsequently, the original word x_i is replaced with a word \tilde{x}_i whose embedding $\phi(\tilde{x}_i)$ is closest to the $\tilde{\phi}_i$ within the embedding space. The previous framework of the word-level DP satisfies ϵd -MetricDP, where $d: \mathcal{X} \times \mathcal{X} \rightarrow \mathbb{R}_+$ is a distance defined within sentence space (e.g., in Euclidean metric space, $d(\mathbf{x}, \mathbf{x}') = \sum_{i=1}^n \|\phi(x_i) - \phi(x'_i)\|$ for \mathbf{x} and \mathbf{x}' with the same length).

Sentence-level DP approaches. Compared to the word-level DP, the sentence-level DP aims to achieve DP at the full document rather than a single word. A common approach is to leverage LMs for paraphrasing tasks to achieve DP [41], [57]. Given a private text \mathbf{x} , the prompt for paraphrasing is constructed by prompt template \mathbf{p}_T and \mathbf{x} . In an autoregressive language model, the output logit in the last layer of the decoder is denoted as $\mathbf{u} \in \mathbb{R}^{|\mathcal{V}|}$ when modeling the next token. To limit the sensitivity, the logit is clipped as $\bar{\mathbf{u}} = \text{CLIP}(\mathbf{u}, C)$, where the clipping function is $\text{CLIP}(\mathbf{u}, C) = \mathbf{u} \cdot \min(1, C/\|\mathbf{u}\|)$. The probability for each word in the vocabulary is computed as $P_j = \text{SOFTMAX}(\bar{\mathbf{u}}) = \exp(\bar{u}_j/T) / \sum_{j=1}^{|\mathcal{V}|} \exp(\bar{u}_j/T)$, where T represents the temperature for controlling randomness level of output. The next token is sampled from the conditional probability distribution P over the vocabulary \mathcal{V} . Note that the sampling procedure can be viewed as the exponential mechanism [42], and the temperature is related to the privacy budget. Given the output length m , the clipping constant C , the paraphrasing procedure is $2mC\epsilon/T$ -LDP following the exponential mechanism.

C. Large Language Models Used in the Experiments

For the LLMs being the targets of the black-box attacks, we use the following models in our experiments.

- **LLaMA** [54], [9] is a family of pre-trained and fine-tuned large language models developed by Meta with 7B to 70B parameters, where the models are over-trained on trillions of tokens from the publicly available data. Note that the details of training data are not been disclosed by model developers. We conducted our experiments on fine-tuned LLaMA-2 with 7B, 13B and 70B parameters and fine-tuned LLaMA-3 with 8B and 70B parameters.
 - **Gemma** [53] is a collection of lightweight pre-trained and fine-tuned decoder-only large language models developed by Google. In our experiments, we employ fine-tuned Gemma-2 with 9B and 27B parameters.
 - **ChatGPT** [7], developed by OpenAI, is provided via black-box APIs for conversation and interaction. Note that OpenAI did not disclose information about the model architecture, training algorithm, and training data. In our experiments, we employ ChatGPT-3.5, ChatGPT-4, and ChatGPT-4o for evaluation.
 - **Claude** [11], released by Anthropic AI, is available via black-box APIs similar to ChatGPT. There are three versions for Claude-3, Haiku, Sonnet, and Opus, where each version is optimized for different tasks. Recently, Anthropic AI also released Claude-3.5 (Sonnet). In our experiments, we employ both four versions for evaluation.
- For the LLMs being the target of our white-box attacks, we use the following famous open-sourced LLMs.
- **OPT** [63] is a family of pre-trained language models using a decoder-only transformers architecture developed by Facebook. Pile is one of the pre-training datasets of OPT, where Pile-CC and Pile-Wiki are included. In our experiments, we employ OPT with 350M, 1.3B and 6.7B parameters.
 - **GPT-Neo & GPT-J** [15], [59], released by EleutherAI, is a collection of transformer-based language models pre-trained on the Pile dataset. In our experiments, we employ GPT-Neo with 1.3B, 2.7B parameters and GPT-J with 6B parameters.
 - **Pythia** [13], released by EleutherAI, is a collection of language models pre-trained on the Pile dataset. In our experiments, we employ Pythia with 1.3B, 2.8B and 6.9B parameters.

D. Ethical Considerations

Our research is intended to enhance the security of deployed systems by helping stakeholders better understand the causes of privacy issues in AI models. Our findings could inform users and designers of such a potential vulnerability, so that more comprehensive privacy solutions can be taken in the future.

We only attempt to infer training data generated by LLMs; no attempt was made to further infer private and sensitive data exposure from LLMs. Furthermore, we make no attempt to de-anonymize any inferred training data. Our work aligns with the ethical guidelines of the Menlo Report, as we not only explain the reasons behind model about privacy leakage and propose

basic defense methods through detection but also offer new insights for future enhancements in privacy protection.

Specifically, this paper discovered the capability of the modern large language models (LLMs) on recovering private content from differentially private prompts where the private information was sanitized. Such findings were based on experiments over the publicly available data and the open APIs to publicly available LLMs (see details in Section V). We faithfully followed the Terms of Service of LLMs when interacting with the LLMs. Since it was believed that differentially private outputs were not invertible, our work might have the following negative outcomes for public interests.

- Disclosure. We discovered a vulnerability in the existing privacy-preserving technique of differential privacy. According to the paper, adversaries could use the latest implementations of LLMs to recover historical data that was intended to be protected by differential privacy. To mitigate this vulnerability, we discussed potential solutions in Section VII.

Overall, we did not engage in any malicious activities, such as exposing sensitive information, disrupting legitimate services, or causing financial or reputational harm to the LLM vendors providing these services.