Abstract

A wave of recent language models have been powered by large collections of natural language datasets. The sudden race to train models on these disparate collections of incorrectly, ambiguously, or under-documented datasets has left practitioners unsure of the legal and qualitative characteristics of the models they train. To remedy this crisis in data transparency and understanding, in a joint effort between experts in machine learning and the law, we've compiled the most detailed and reliable metadata available for data licenses, sources, and provenance, as well as fine-grained characteristics like language, text domains, topics, usage, collection time, and task compositions. Beginning with nearly 40 popular instruction (or “alignment”) tuning collections, we release a suite of open source tools for downloading, filtering, and examining this training data. Our analysis sheds light on the fractured state of data transparency, particularly with data licensing, and we hope our tools will empower more informed and responsible data-centric development of future language models.

1. Introduction

The latest wave of language models, both public (Chung et al., 2022; Taori et al., 2023; Geng et al., 2023) and proprietary (including Bard Anil et al., 2023, ChatGPT Ouyang et al., 2022, GPT-4 OpenAI, 2023), are capable of a range of general reasoning abilities (Wei et al., 2022). This is attributed in large part to the diversity and richness of their training data, including pre-training corpora, and finetuning datasets paired with instructions (Wei et al.; Sanh et al., 2021) or human feedback (Ouyang et al., 2022). Natural language training data is comprised of hundreds of data sources, both for pre-training (Gao et al., 2020), and for instruction tuning, as compiled by academics (Wang et al., 2022b; Longpre et al., 2023a; Muennighoff et al., 2022), synthetically generated by models (Taori et al., 2023; Wang et al., 2022a), or aggregated by platforms like Hugging Face (Lhoest et al., 2021).

A Crisis in Data Transparency

A central challenge to model developers is crowd-sourcing quality collections of data, with reliable information on their contents and limitations (Longpre et al., 2023b). Recent trends have seen massive collections with sparser documentation and attribution (Wang et al., 2022c), a lack of Dataset Cards or Datasheets (Gebru et al., 2021; Pushkarna et al., 2022), even non-disclosure of training sources (OpenAI, 2023; Anil et al., 2023), and ultimately a decline in understanding the raw training data mixtures (Dodge et al., 2021). This lack of understanding can lead to data leakages between training and test data, or exposing personally identifiable information (PII) (Bubeck et al., 2023), poor quality models than anticipated, and unintended biases or behaviours (Welbl et al., 2021; Xu et al., 2021). The Data Provenance effort aims to remedy this deterioration in data documentation by compiling relevant metadata for thousands of popular datasets (a large undertaking), and expanding their metadata with a much richer taxonomy than Hugging Face, Papers with Code, or other aggregators. To empower better data documentation and understanding, we provide tools to (a) filter, download, and explore data collections, but also (b) auto-generate a Data Provenance Card, as a supplement to Datasheets (Gebru et al., 2021) for sections on data sourcing and composition.

Unreliable Data Provenance & Licensing

Our annotation collection process revealed systemic problems particularly data licenses, where existing aggregations are a mix of sparse, ambiguous, and incorrect. For instance, 513 of Super-Natural Instruction’s 1556 tasks having “Unknown” licenses (Wang et al., 2022b), leaving a substantial information gap. As a result, much of this data is unusable for risk-averse or non-academic practitioners. Second, the annotations that are collected are often incorrect—we randomly sampled 84 datasets with HuggingFace URLs, and found 49% were incorrectly labeled, usually as more per-
missive. Third, ambiguously licensed datasets, such as ShareGPT (Vercel, 2023) and Alpaca (Taori et al., 2023), which leverage generations from proprietary models, have been commonly adopted, with developers only realizing the ramifications after their models are fully trained and even deployed. These informational gaps, ambiguities, and license mis-transcriptions have led to misapprehensions (eg. LMSYS-Org (2023) claiming models are “compatible with commercial usage” despite Flan-T5 finetuning on datasets licensed as Non-Commercial), license revisions post-public release (with MPT-StoryTeller (Frankle, 2023)), and even lawsuits (eg. Stability AI (Arstechnica, 2023)).

Uncertainty in legal interpretations (Section 3) means practitioners rely on many signals beyond licenses to decide their risk tolerance in using a training dataset. Discussion with practitioners revealed these signals include the dataset creators, the original data sources, as well as precedence of use (downloads and citations). With legal experts, we design a pipeline for tracing dataset provenance, including their original sources, their licenses, and subsequent use.

The legal treatment of training data has significant consequences on AI development. Records in training data are normally copyrighted, and it remains unclear if the process of converting training data into model weights violates the copyrights of the original authors (Quang, 2021; Epstein et al., 2023). Using copyrighted training data may be considered “fair use” because the use of copyrighted material is far from the original purpose of the material (Sobel, 2017). Independent of these open legal questions, a transparent chain of provenance for data contributes to transparent and responsible AI development. To this end, the Data Provenance Project helps developers clearly attribute the data they use. We enumerate our contributions:

1. **Designing Large-scale Data Documentation** A combined human-machine data documentation framework, designed by legal and AI experts, to collect reliable information on dataset licenses, characteristics and provenance.

2. **The First Empirical Analysis of Natural Language Dataset Licenses** This work comprises the first large scale, empirical comparison of data licensing practices for natural language datasets.

3. **Tools for Data Provenance** An open source repository for downloading, filtering, and exploring detailed properties of thousands of text datasets. This includes tools to auto-generate Data Provenance Cards for future documentation best practices.

2. **The Data Provenance Project**

The Data Provenance Project remedies the described challenges with a large-scale expert-guided annotation of popular text datasets. We tailor our annotations, described in Section 2.1, to characteristics relevant for designing a well-informed training corpus. To begin with we target nearly 40 popular instruction or “alignment” finetuning data collections, for which we list a few examples in Table 1.

### 2.1. Data on Data

Our information collection spans (I) identifier information, bridging metadata from several aggregators, including Hugging Face, Papers with Code, Semantic Scholar, and ArXiv, (II) detailed dataset characteristics for a richer understanding of training set composition, and (III) dataset provenance for licensing and attribution. Our repository of tools then allow practitioners to filter data on any of the listed criteria and visualize the other characteristics of the resulting data. For their selected criteria they may then generate a human readable, markdown summary, or “Data Provenance Card” of the used datasets, and their compositional properties for languages, tasks, and licenses.

#### Identifier Information

1. **Dataset Identifiers**: The dataset’s name, associated paper title, and description of the dataset.

2. **Dataset Aggregator Links**: A link each major aggregator, including Hugging Face, Papers with Code, Semantic Scholar, and ArXiv allows us to incorporate and compare their crowdsourced metadata.

3. **Collection**: The name and URL to the data collection of which this dataset is apart.

#### Dataset Characteristics

1. **Languages**: Each of the languages represented in the dataset. We use automated methods to augment language identification, as aggregators are often sparse.

2. **Task Categories**: The 20+ task categories represented in the instructions, such as Question Answering, Translation, Program Synthesis, Toxicity Identification, Creative Writing, and Roleplaying.

3. **Text Topics**: An automated annotation of the topics discussed in the datasets.

4. **Text Length Metrics**: The minimum, maximum, and mean number of dialog turns per conversation, of characters per user and per assistant.

5. **Format**: The format and intended use of the data. The options are zero-shot prompts, few-shot prompts, chain-of-thought prompts, multi-turn dialog, and response ranking.

6. **Time of Collection**: The time as which the work was published, which acts as an upper bound estimate on the age of the text.
Dataset Provenance

1. **Licenses**: The license name and URLs associated with the data, using the process described in Section 2.2
2. **Text Source**: The original sources of the text, often Wikipedia, Reddit, or other scraped online/offline sources.
3. **Creators**: The institutions of the dataset authors, including universities, corporations, and other organizations.
4. **Attribution**: The attribution information for the authors of the paper associated with the dataset.
5. **Citation & Download Counts**: The citation and Hugging Face download count for the paper and dataset, dated June 2023. This acts as an estimate or community use, and is commonly used as precedence to decide on the risk-level for using these datasets when the license is Unspecified.

2.2. Data Provenance Collection

This data was collected with a mix of manual and automated techniques. Connecting disparate dataset information hubs, like Github, Hugging Face and Semantic Scholar, required manual search. Annotating and verifying license information, in particular, required a carefully guided manual workflow, designed with legal practitioners. Once these information hubs were connected, it was possible to synthesize or scrape additional metadata, such as dataset languages, task categories, and time of collection. And for richer details on each dataset, like text topics and source, we used carefully tuned prompts on language models inspecting each dataset.

**Automated Annotation Methods** Based on the manually retrieved pages, we automatically extract Licenses from HuggingFace configurations and GitHub pages. We leverage the Semantic Scholar public API (Kin, 2023) to retrieve the released date and current citation counts associated to academic publications. Additionally, we compute a series of other helpful, but often overlooked data properties such as text metrics, and dialog turns. We elected to measure sequence length in characters rather than word tokens, for fairer treatment by language and script.

**API Annotation Methods** While task categories have been the established measurement of data diversity in recent instruction tuning work (Sanh et al., 2021), they omit other perspectives on data diversity and representation. To augment this, we use OpenAI’s ChatGPT API to help annotate for richer text features. We randomly sampled 100 examples per dataset and carefully curated model prompts (with examples) to suggest up to 3 topics discussed in the text.

To annotate for the original data sources, we embedded the text from the dataset’s academic paper into a prompt for ChatGPT’s API. Our manual verification of these prompts and their answers showed reliable and accurate results for simple tasks like topic classification, language identification, and keyword extraction (data sources).

**License Annotation Workflow** Natural language datasets are often combined into large collections which can make some of the requirements of open-source licenses challenging to operationalize. Machine learning practitioners usually

---

**Figure 1.** The metadata collection pipeline, combining manual and automatic processes.
want to segment these datasets into categories, representing whether they are allowed to train on the data, evaluate on it, modify it, and/or re-distribute it. Our license annotation workflow follows these steps:

1. **Compile all License Information** We aggregate all licensing information from Github, ArXiv, Hugging Face, Papers with Code, and the collection itself (e.g. Super-Natural Instructions).

2. **Search for explicit Data Licenses** The human annotator searches for a license specifically given to the dataset (not the code) by the authors. A license is found if (a) the Github repository mentions or links a license for the data, (b) the Hugging Face Dataset Card mentions or links a license for the data, (c) the Hugging Face license label was uploaded by the dataset creator themselves, (d) a dataset-specific license is linked from Papers with Code, or the paper itself.

3. **Identify a License Type** A license may fall into a set of common categories (e.g. MIT, Apache 2, CC BY SA, etc.), be a “Custom” license, a permission Request Form, or if none was found for the data, “Unspecified”. If a dataset is comprised of multiple parts, the annotator can label a list of license types. The license type is accompanied by a license URL and license notes from the annotator, for posterity and categorizing “Custom” licenses (the next step).

4. **Categorize Licenses** Based on discussions with industry experts, we categorize licenses based on four important features: is data usage limited to academic or non-commercial purposes (**Permitted Use**), does the data source need to be attributed (**Attribution**), and do derivatives of the data need to licensed under the the same terms as the original (**Share-Alike**).

5. **Additional Provenance** In practice, legal teams may wish to balance their risk tolerance with more nuanced criteria. For instance, they may be satisfied with using (more permissive) Github licenses, even when it is ambiguous whether these apply to the code or the data. They may also wish to include or exclude datasets based on whether these are widely used in practice, where the original data was sourced from, and if the creator is a competitor. To supplement the above license categories, we also collect all this metadata for filtering.

Even these simple steps raise challenges: for example, the attribution clauses of many licenses require a copy of the original license to be included with the licensed material. For a large collection, this could mean that thousands of different licenses would need to be attached to a trained model. Our project aims to comply with the terms of license agreements while also focusing on pragmatic usability. For example, to resolve the issue of attribution, we assemble a master list of licenses for each user’s request and also create a more concise data card that attributes datasets more concisely and conveniently.

### 3. Legal Discussion

The legal landscape surrounding the use of alignment data is complex. It remains unclear how license terms should be interpreted for data usage and many relevant laws, including copyright and fair use, are ill-defined in this context.

Most open source licenses were designed for software, but we find them being attached to alignment data. These licenses were not originally conceived with data utilization in mind, rendering their terms ambiguous when applied to this new context. This issue is further exacerbated when multiple datasets, each potentially governed by a different open-source license, are amalgamated into collections. A primary concern arises in determining whether machine learning models trained on these data collections should be classified as “derivative” works. If so, such models would, for example, be subject to copyleft requirements, which may preclude developers from utilizing multiple datasets released under incompatible copyleft licenses or require them to assemble hundreds or thousands of licenses to satisfy attribution requirements.

If license terms are deemed to be inapplicable to data, datasets may nevertheless be protected under copyright laws. This situation offers some potential legal avenues for data utilization, such as statutory exceptions - exemplified by the European Union’s Data Mining exception - or fair use standards. Yet again, the application of these exceptions and standards to machine learning remains ill defined, further complicated by jurisdictional differences in legal standards.

In the face of these pervasive legal uncertainties, practitioners’ decisions regarding data usage are ultimately guided by a blend of factors including the specific licensing terms, the origin of datasets, and the degree of usage of a given dataset by others. Navigating this landscape requires striking a delicate balance between risk mitigation and the need for sufficient resources. This equation, however, varies across regions, applications, and corporate environments, influenced by factors such as competition, risk, and regional legislation.

In creating a repository of all this information, we hope to give practitioners the ability to make informed choices, while encouraging dataset creators with the ability to be more thoughtful about the licenses that they select. Ultimately, data licenses could be leveraged to promote more responsible, inclusive, and transparent machine learning practices.
References


A. Data Collections

In the Data Provenance Project we compile nearly 40 collections of instruction and alignment tuning datasets. A subset of these are listed in Table 1 to illustrate the diversity in source, characteristics, languages, and licenses. It also illustrates the focus on popular and commonly used datasets in the community.
Table 1. **Alignment Tuning Collections and their characteristics.** For data taken from proprietary sources, we annotate with OpenAI’s Non-compete (OAI NC) clause, or with Reddit’s API terms.