AI Confidentiality & Accuracy. Together at Last.

Retain Data Ownership and Confidently use AI with Protopia AI's Stained Glass Transform

PROTOPIA®

Enable Safe Access for AI: Stained Glass Transform

Protopia AI's Stained Glass Transform™ (SGT) enables enterprises to harness the power of cutting-edge ML solutions without giving up data ownership. Stained Glass transforms unprotected data into a **Randomized Re-Representation** that is still usable for ML training and inference. This stochastic version of your data still holds the information needed for the AI tasks but not in its original, human-readable representation.

Stained Glass for Large Language Models (LLM)

For Enterprise LLM users Stained Glass Transform™ helps enterprises use advanced LLMs while retaining ownership of their sensitive data. You can prompt an already-trained LLM through Stained Glass created by the LLM provider. You can also holistically transform your fine-tuning data so that your provider can train models for you without exposure. Protect your data both when using hosted models, as well as internally deployed models shared among enterprise departments. Below are two LLM prompting and fine-tuning examples.
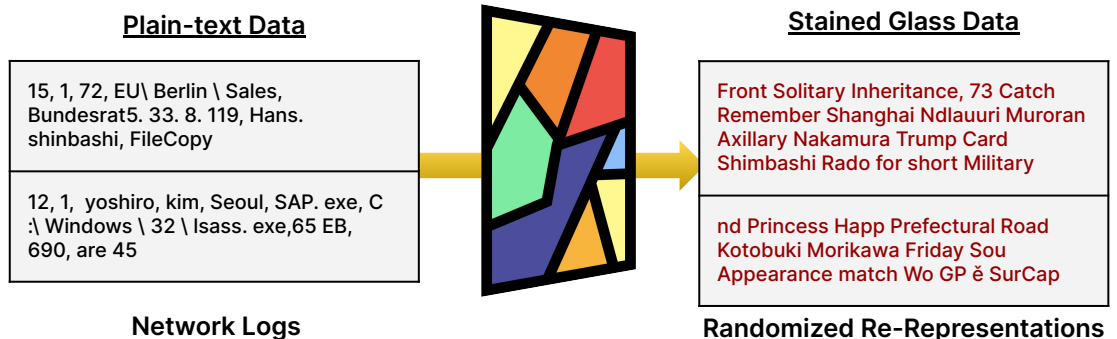
LLM Prompting

Plain-text Data	Stained Glass Data
Question: What are the name of my cats? **Context:** I have two beautiful cats named Maria and Oliver. One is black the other is white and grey. They like to play together and sleep for most of the day.	**Question and Context:** awokenuk wingCNNcancer Nebula digitgelismaMagikarpinducing Franken PowersgeraldWra beansrxizonSportacht dreams ICEublicobilabad technvgodeundown lur outweMinnes otasellasciheelsactorildboroughsequent RidingKEYnatureconservancynoticeissance
Generated Response: Maria and Oliver	**Generated Response: Maria and Oliver**

The left shows a prompt to the LLM, "Maria & Oliver" as the response. The right shows that the text can't be reconstructed from the transformed prompt, but the LLM generates the correct response.

LLM Fine-Tuning: Customer Example for Network Log Analysis

The transformed, uninterpretable data on the right was used to fine-tune the LLM, achieving near identical performance as with unprotected data.

Plain-text Data

15, 1, 72, EU\ Berlin \ Sales, Bundesrat5. 33. 8. 119, Hans. shinbashi, FileCopy

12, 1, yoshiro, kim, Seoul, SAP. exe, C :\ Windows \ 32 \ lsass. exe,65 EB, 690, are 45

Network Logs

Stained Glass Data

Front Solitary Inheritance, 73 Catch Remember Shanghai Ndlauuri Muroran Axillary Nakamura Trump Card Shimbashi Rado for short Military

nd Princess Happ Prefectural Road Kotobuki Morikawa Friday Sou Appearance match Wo GP ě SurCap

Randomized Re-Representations

For LLM Providers Generate Stained Glass Transform for your most generalizable and efficient hosted models without needing access to unprotected confidential enterprise data.

Integrating Stained Glass
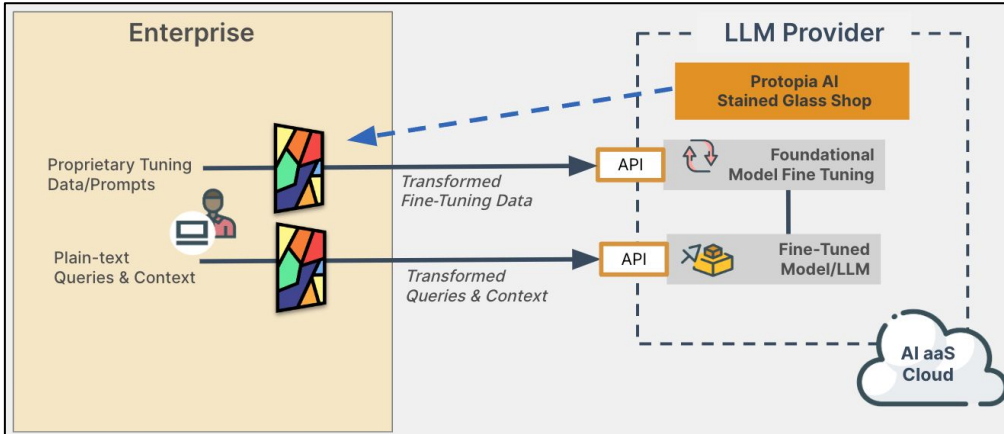
LLM providers can run Protopia AI without altering the training process of their LLMs. The created transformation is subsequently run on the enterprise side to protect the plain-text prompts and/or fine-tuning data.

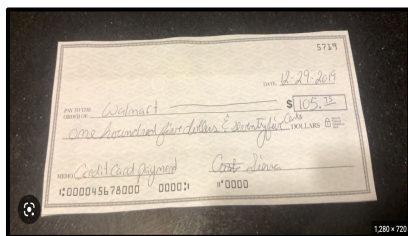## Stained Glass Transform with Visual Data

SGT has been tested in a variety of visual, tabular, and textual use-cases in financial services, manufacturing, defense. The images below highlight examples demonstrated to the US Navy and financial services company Q2. In both examples, a pre-trained AI model was shown to accurately make inferences/predictions using transformed data on the right, instead of needing to access unprotected plain data on the left.

Unleashing Enterprise Data for GenAI and LLMs

With the risk of leaking sensitive and confidential information, data protection has become a top enterprise adoption barrier. Bold innovation to accelerate and ensure safe usage iof technical solutions is the way forward. Enterprises need to:

Maintain and Secure Data Ownership

Tap into the value of enterprise data for AI

Protect Data During training/fine-tuning & inference/prompting

Scan the QR code on page 1 or email info@protopia.ai to meet with and expert.
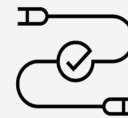
Stained Glass in Defense and Financial Services
Transform data to match intent of model consuming it

US Navy Live VIP Recognition without Protopia AI

Protopia AI enabling VIP recognition on only necessary traits with transformed video stream

Q2 Check Fraud Detection without Protopia AI

Q2 partners with Protopia AI to develop new product that safely uses Randomized Re-Representations of checks