EFTHYMIOS (THEMIS) TSAPRAZLIS

3710 McClintock Ave., RTH 318 ◇ Los Angeles CA, 90089, USA
tsaprazl@usc.edu ◇ timtsapras23.github.io/◇ Google Scholar

RESEARCH INTERESTS

Privacy-Preserving ML, Vision-Language, Generative AI, Computer Vision, Natural Language Processing

EDUCATION

University of Southern California Aug 2024 - present
PhD in Computer Science, advised by Prof. Shrikanth Narayanan *Los Angeles CA, USA*

National Technical University of Athens Sep 2018 - July 2024
BSc and MEng in Electrical and Computer Engineering *Athens, Greece*
Thesis: *Enhancing contrastive language-vision pre-training with generative dialogue*, supervised by Prof. Petros Maragos

RESEARCH EXPERIENCE

Signal Analysis and Interpretation Lab, USC Aug 2024 - present
Graduate Research Assistant *Los Angeles CA, USA*
Performing research on privacy-preserving machine learning.

University of Texas at Austin Nov 2022 - Aug 2024
Research Student *Austin TX, USA*
Performed research on contrastive learning for vision-language pretraining advised by Prof. Alex Dimakis.

Computer Vision and Signal Processing Group, NTUA
Robot Perception and Interaction Unit, Athena RC Jan 2024 - July 2024
Research Assistant *Athens, Greece*
Performed research on lifelong learning for robotic agents as part of the PILLAR-Robots project.

National Technical University of Athens Nov 2022 - July 2024
Undergraduate Research Assistant *Athens, Greece*
Performed research on self-supervision and contrastive learning.

NCSR "DEMOKRITOS" Sep 2022 - Nov 2022
Research Intern *Athens, Greece*
Developed an end-to-end framework for multimodal sentiment analysis.

PROFESSIONAL EXPERIENCE

Workable Software Oct 2023 - Dec 2023
Machine Learning Engineer Intern *Athens, Greece*
Performed research on visual information extraction on documents such as resumes.

TALKS

1. **4th Annual Symposium of USC-Amazon Center**
   Talk: *Assessing Visual Privacy with VLMs*
   May 2025, Los Angeles, CA

AWARDS

1. **USC–Amazon Center on Secure and Trusted Machine Learning Gift Award, 2025**.
   Competitive seed grant supporting research on privacy-preserving and trustworthy AI.
2. **Thomaides Award for Scientific Publications, 2025**
   Recognized for outstanding research publications in 2023 during undergraduate studies.
3. **ARISE Stipend Award, 2021**
   Full tuition coverage for participation in the EIT Digital Summer School 2021.

PUBLICATIONS

- **Efthymios Tsaprazlis**, Tiantian Feng, Anil Ramakrishna, Rahul Gupta, Shrikanth Narayanan. Assessing Visual Privacy Risks in Multimodal AI: A Novel Taxonomy-Grounded Evaluation of Vision-Language Models. *arXiv preprint arXiv:2509.23827*, 2025.
- **Efthymios Tsaprazlis**, Thanathai Lertpetchpun, Tiantian Feng, Sai Praneeth Karimireddy, Shrikanth Narayanan. VoxGuard: Evaluating User and Attribute Privacy in Speech via Membership Inference Attacks. *arXiv preprint arXiv:2509.18413*, 2025.
- Panagiotis P Filntisis, **Efthymios Tsaprazlis**, Paraskevas Oikonomou, Francesco Mattioli, Vieri Giuliano Santucci, George Retsinas, and Petros Maragos. Towards Open-ended Robotic Exploration using Vision-Inspired Similarity and Foundation Models. *2025 IEEE International Conference on Robotics and Automation (ICRA), Atlanta, USA*, 2025.
- **Efthymios Tsaprazlis**, Georgios Smyrnis, Alex Dimakis, and Petros Maragos. Enhancing CLIP with a Third Modality. *In NeurIPS 2023 Workshop: Self-Supervised Learning - Theory and Practice*, 2023.

SUMMER SCHOOLS

Lisbon Machine Learning School (LxMLS) 2022 Jul 2022
Instituto Superior Technico (IST) *Lisbon, Portugal*

Topics: *Probability Theory & Linear Algebra, Linear Classifiers, Neural Networks, Sequence Models, Neural Structured Models, Causality.*

EIT Digital Platforms for Industry 4.0 Jul 2021 - Aug 2021
Technical University of Munich *Munich, Germany*

Developed a video surveillance framework for industrial environments monitoring with computer vision.

SKILLS

Programming Languages	**Python**, MATLAB /SIMULINK, C/C++, SQL,
Tools	**PyTorch**, Bash, Jupyter, Git, TensorFlow
Languages	English(Fluent), Greek(Native)

VOLUNTEERING

IEEE ICASSP 2023 Student Volunteer: Served as a student volunteer in the IEEE 48th International Conference on Acoustics, Speech, and Signal Processing (ICASSP), Rhodes (2023).

RESEARCH PROJECTS

Alignment in Multimodal AI through Explainable Privacy Understanding
USC - Amazon (Sep 2024 - present)

- Received gift award from the USC-Amazon Center on Secure and Trusted Machine Learning
- Introduced a legally grounded taxonomy of visual privacy risks integrating principles from legal frameworks with public expectations, creating a structured foundation for benchmarking multimodal models and guiding dataset design.
- Benchmarked state-of-the-art vision–language models on privacy detection and compliance reasoning tasks, exposing critical limitations in recognizing fine-grained attributes and reason about context-sensitive privacy risks.
- Developing a large-scale dataset derived from the taxonomy and building an end-to-end advisory toolkit to detect, localize, and sanitize sensitive visual content, aiming to both advance research benchmarks and deliver deployable privacy solutions.

Context-Aware Anonymization
USC (February 2025 - present)

- Proposed and built a benchmark and synthetic dataset to disentangle privacy-sensitive scenarios into parallel information flows, preserving higher utility vs CI baselines and enabling selective remediation with more explainable privacy enforcement.
- Revealed LLMs are overly conservative in privacy judgments, often blocking legitimate information, and demonstrated flow-based reasoning enables selective remediation that better balances privacy with communication needs.
- Planning to design contextual auditors and anonymizers that detect hidden attributes, decompose conversations into sensitive flows, and apply targeted transformations, for practical privacy protection in domains such as healthcare and legal communication.

Privacy Trade-offs in Speech Processing
USC (May 2025 - present)

- Reframed speaker and attribute verification as membership inference attacks, showing that models with similar EER can leak up to 100× more at low-FPR, where attackers make reliable predictions, revealing that standard metrics hide true privacy risks.
- Investigating trade-offs in speech anonymization across privacy, downstream utility, perceptual quality, and computational cost.

IARPA HIATUS
USC ISI - UMD - UMich - UBirmingham (Aug 2025 - present)

- Define and lead the lab's research agenda on authorship privacy for a multi-institution IARPA program; coordinate technical efforts, drive project next-steps, and present findings directly to IARPA program managers and partners.
- Building a spoken language privacy benchmark for attribute prediction, evaluating LLMs as both predictors and anonymizers, measuring privacy leakage with DP-inspired metrics, and analyzing style shifts from original to generated text.