Sixth Workshop on Privacy in Natural Language Processing (PrivateNLP 2025)

Albuquerque, New Mexico, USA
4 May 2025

ISBN: 979-8-3313-1926-7

Printed from e-media with permission by:

Curran Associates, Inc.
57 Morehouse Lane
Red Hook, NY 12571



Some format issues inherent in the e-media version may also appear in this print version.

Copyright© (2025) by the Association for Computational Linguistics
All rights reserved.

Printed with permission by Curran Associates, Inc. (2026)

For permission requests, please contact the Association for Computational Linguistics
at the address below.

Association for Computational Linguistics
209 N. Eighth Street
Stroudsburg, Pennsylvania 18360

Phone: 1-570-476-8006
Fax: 1-570-476-0860

acl@aclweb.org

Additional copies of this publication are available from:

Curran Associates, Inc.
57 Morehouse Lane
Red Hook, NY 12571 USA
Phone: 845-758-0400
Fax: 845-758-2633
Email: curran@proceedings.com
Web: www.proceedings.com

Table of Contents

TUNI: A Textual Unimodal Detector for Identity Inference in CLIP Models
Songze Li, Ruoxi Cheng and Xiaojun Jia 1

TAROT: Task-Oriented Authorship Obfuscation Using Policy Optimization Methods
Gabriel Loiseau, Damien Sileo, Damien Riquet, Maxime Meyer and Marc Tommasi 14

Balancing Privacy and Utility in Personal LLM Writing Tasks: An Automated Pipeline for Evaluating Anonymizations
Stefan Pasch and Min Chul Cha 32

Named Entity Inference Attacks on Clinical LLMs: Exploring Privacy Risks and the Impact of Mitigation Strategies
Adam Sutton, Xi Bai, Kawsar Noor, Thomas Searle and Richard Dobson 42

Inspecting the Representation Manifold of Differentially-Private Text
Stefan Arnold 53

Beyond Reconstruction: Generating Privacy-Preserving Clinical Letters
Libo Ren, Samuel Belkadi, Lifeng Han, Warren Del-Pinto and Goran Nenadic 60

Beyond De-Identification: A Structured Approach for Defining and Detecting Indirect Identifiers in Medical Texts
Ibrahim Baroud, Lisa Raithel, Sebastian Möller and Roland Roller 75

Investigating User Perspectives on Differentially Private Text Privatization
Stephen Meisenbacher, Alexandra Klymenko, Alexander Karpp and Florian Matthes 86