Zhiping (Arya) Zhang

Email: zhang.zhip@northeastern.edu   **Website:** zhipingzhang.com   Google Scholar

My research focuses on 1) understanding privacy challenges in (personalized) agentic AI systems;
and 2) leveraging effective Human-AI collaboration (e.g., supporting human autonomy)
to align AI behavior with individuals' privacy preferences in real-world applications.

Education	**Ph.D. student in Computer Science** *Northeastern University (NEU), Supervisor: Prof. Tianshi Li*	Boston, US 2024 - 2029 (Exp.)
	M.Sc. in Industrial Design (HCI Track) *Eindhoven University of Technology (TU/e)*	Eindhoven, Netherlands 2018 - 2020
	B.Eng. in Industrial Design (Honours, Top 1) *University of Liverpool (UoL), Xi'an Jiaotong-Liverpool University*	China & UK 2014 - 2018

Research Experience	**Privacy-Enabling AI & Computer-Human Interaction Lab** Conducted human-centered privacy research on language models and agentic AI systems using mixed methods, system building, and computational experiments. First-authored papers published in CHI '24 [C.2], CSCW '25 [C.3], and submitted to CHI '26 [I.1]. (Advised by *Prof. Tianshi Li*)	2024 - present
	CompLING Lab-AI Group, UWaterloo Led a project on mitigating privacy concerns in personalized LM agents by balancing human control and agent autonomy. Developed an LLM agent system and conducted a computational experiment. First-authored paper submitted to CHI '26 [I.2]. (Advised by *Prof. Freda Shi*)	Summer 2025
	Social Robotics Lab, TU/e Worked on social robot role design, robot behavior programming, and conducted a field test. Co-authored paper published in HRI '20 [C.1]. (Advised by *Prof. Emilia Barakova & Panos Markopoulos*)	2019

Industry Experience	**AI Product Manager**, *Fiture* Explored AI-powered home gym equipment, bridging algorithms and real products (*a voice assistant*, *natural language & body-pose remote control*, and *a course searching and recommendation system*).	2021 - 2023
	User Experience Design & Research, *Alibaba* Researched and designed user experience to support multi-role collaboration in enterprise purchasing systems. (*an intelligent purchasing conversational agent*: enhanced purchasers' workflow and increased user satisfaction by 22% after launch).	2020 - 2021

* indicates co-first authorship.

Peer-reviewed conference and journal papers

[C.3] **Secret Use of Large Language Model (LLM)**
Zhiping Zhang, Chenxinran Shen, Bingsheng Yao, Dakuo Wang, Tianshi Li.
In Proceedings of the ACM on Human-Computer Interaction (CSCW '25)

[C.2] **"It's a Fair Game", or Is It? Examining How Users Navigate Disclosure Risks and Benefits When Using LLM-Based Conversational Agents**
Zhiping Zhang, Michelle Jia, Hao-Ping (Hank) Lee, Bingsheng Yao, Sauvik Das, Ada Lerner, Dakuo Wang, Tianshi Li.
In Proceedings of the CHI Conference on Human Factors in Computing Systems (CHI '24)

[C.1] **Robot role design for implementing social facilitation theory in musical instruments practicing**
Heqiu Song, *Zhiping Zhang*, Emilia I. Barakova, Jaap Ham, Panos Markopoulos
In Proceedings of the 2020 ACM/IEEE International Conference on Human-Robot Interaction (HRI '20).

In Submission

[I.2] **Autonomy Matters: A Study on Personalization-Privacy Dilemma in LLM Agents**
Zhiping Zhang, Yi Evie Zhang, Freda Shi, Tianshi Li (CHI '26)

[I.1] **Privacy Leakage Overshadowed by Views of AI: A Study on Human Oversight of Privacy in Language Model Agent**
Zhiping Zhang, Bingcan Guo, Tianshi Li (CHI '26)

SIG/Poster/ Workshop

[W.1] **Toward a Human-centered Evaluation Framework for Trustworthy LLM-Powered GUI Agents**
Chaoran Chen*, *Zhiping Zhang**, Ibrahim Khalilov, Bingcan Guo, Simret A Gebreegziabher, Yanfang Ye, Ziang Xiao, Yaxing Yao, Tianshi Li, Toby Jia-Jun Li (HEAL @CHI '25)

[P.1] **The Obvious Invisible Threat: LLM-Powered GUI Agents' Vulnerability to Fine-Print Injections**
Chaoran Chen, *Zhiping Zhang*, Bingcan Guo, Shang Ma, Ibrahim Khalilov, Simret A Gebreegziabher, Ziang Xiao, Yaxing Yao, Tianshi Li, Toby Jia-Jun Li (SOUPS '25)

[S.1] **Human-Centered Privacy Research in the Age of Large Language Models**
Tianshi Li, Sauvik Das, Hao-Ping (Hank) Lee, Dakuo Wang, Bingsheng Yao, *Zhiping Zhang*
In Proceedings of the CHI Conference on Human Factors in Computing Systems (CHI '24)

Professional Service	**Program Committee**
	2026: AgentCraft @IUI '26
	2025: HAIPS @CCS '25, ACM Conference on Intelligent User Interfaces (IUI '26)

External Reviwer

✿ *Received "special recognitions" for outstanding reviews*

2025: CHI '26, IUI '26, HRI '26, IMWUT '25, UIST '25, TEI '25, IJHCS

2024: ✿ CHI '25, CSCW '24, CUI '24

Awards		
	IF Design Award Winner	2024
	Reddot Award Winner	2023
	IF Talent Award Winner	2020
	Alibaba High-level Talents Scholarship	2020
	China-U.S Young Maker Competion Final Excellence Award	2018
	Best Overall Academic Performance (Top 1)	2018
	Academic Achievement Award Scholarship (Top 5%)	2018
	Academic Excellence Award Scholarship (Top 10%)	2017
	COMAP's Interdisciplinary Contest in Modeling - Achievement Meritorious Winer (Top 5%)	2016