Leveraging Large Language Models (LLMs) to Support Collaborative Human-AI Online Risk Data Annotation

JINKYUNG PARK, Vanderbilt University, USA PAMELA WISNIEWSKI, Vanderbilt University, USA VIVEK SINGH, Rutgers University, USA

In this position paper, we discuss the potential for leveraging LLMs as interactive research tools to facilitate collaboration between human coders and AI to effectively annotate online risk data at scale. Collaborative human-AI labeling is a promising approach to annotating large-scale and complex data for various tasks. Yet, tools and methods to support effective human-AI collaboration for data annotation are under-studied. This gap is pertinent because co-labeling tasks need to support a two-way interactive discussion that can add nuance and context, particularly in the context of online risk, which is highly subjective and contextualized. Therefore, we provide some of the early benefits and challenges of using LLMs-based tools for risk annotation and suggest future directions for the HCI research community to leverage LLMs as research tools to facilitate human-AI collaboration in contextualized online data annotation. Our research interests align very well with the purposes of the LLMs as Research Tools workshop to identify ongoing applications and challenges of using LLMs to work with data in HCI research. We anticipate learning valuable insights from organizers and participants into how LLMs can help reshape the HCI community's methods for working with data.

CCS Concepts: • Human-centered computing -> Interactive systems and tools.

Additional Key Words and Phrases: Large Language Model, Research Tool, Human-AI Collaboration, Online Risk Annotation, Conversational Agent

ACM Reference Format:

Jinkyung Park, Pamela Wisniewski, and Vivek Singh. 2024. Leveraging Large Language Models (LLMs) to Support Collaborative Human-AI Online Risk Data Annotation. In *CHI 2024 Workshop on LLMs as Research Tools: Applications and Evaluations in HCI Data Work, May 12, 2024, Honolulu, HI, USA*. ACM, New York, NY, USA, 6 pages.

1 INTRODUCTION

Online risk exposure is a pervasive phenomenon that affects millions of social media users every day [9, 12, 32, 38]. Given the massive scale of online content generation, the development and implementation of machine learning (ML) based risk detection tools to automatically identify and mitigate various online risks has been accelerating (e.g., [5, 14, 24, 27, 28, 33, 35]). To develop these AI-based systems, Human-Computer Interaction (HCI), social computing, and ML research often employ a team of human coders to complete ground-truth data annotations (e.g., classifying whether messages are risky or not) through collaborative tasks among human annotators [2, 7, 20], in which a coding scheme is pre-defined, a group of coders is trained with the scheme to reconcile disagreement, and inter-coder agreement is evaluated [25]. This often includes crowdsourced workers [11], a team of researchers and research assistants [28, 34], and/or domain experts [27]. This annotation process involves an intensive and collaborative process of training, consensus-building, and quality control among multiple coders; therefore, it can be costly, time-consuming, and stress-inducing, while still yielding uneven levels of inter-coder agreement [4, 29].

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the owner/author(s).

© 2024 Copyright held by the owner/author(s).

Manuscript submitted to ACM

Alternatively, proxies are used to label online risk collectively instead of annotating individual risk cases. For instance, existing literature on misinformation detection that relied on source-level labels assumes that all new articles from a given source share the same credibility level (reliable vs. unreliable) depending on the reputation of the source [8, 10, 26]. However, in a recent study, researchers showed only about 50% alignment between source level and article level labels for the credibility of political news articles and called for approaches to balance the quality and quantity of the ground truth annotation [27]. As such, there is a growing need for innovative and efficient methods to support human coders in labeling large corpora of online data, which can have a significant methodological impact on HCI and social computing research. In this position paper, we discuss the potential of the use of Large Language Models (LLMs)-based Conversational Agents (CAs) as AI-based co-coders for accurately annotating online risk data. Our position paper is highly relevant to the LLMs as Research Tools workshop as our focus on LLMs as research tools to facilitate online risk data annotation aligns very well with the core topic of interest for the workshop (i.e., LLMs to reshape the HCI community's suite of methods for working with data).

2 LLMS AS COLLABORATIVE AGENTS FOR ONLINE RISK ANNOTATION

After the recent release of various Large Language Model (LLM)-based Conversational Agents (CAs) (e.g., ChatGPT [21]), research communities are increasingly experimenting with data annotation tasks such as annotating political stance and sentiment of textual data [1, 15, 18, 36]. Emerging literature suggests that LLM-based CAs can be useful for text classification tasks, owing to their accuracy and ability to flexibly adapt to tasks. For instance, Zhang et al. [36] show that ChatGPT was able to annotate the political stance of the tweets with an average accuracy above 70. Similarly, Amin et al. [1] evaluated how accurately ChatGPT classifies sentiment, personality, and suicide ideation in given texts. The results showed that ChatGPT outperformed other robust language models for accurately classifying the sentiment of the text (i.e., positive, neutral, and negative classes). At the same time, challenges have been documented in the use of LLM-based CAs in annotating textual data for more contextualized constructs. For instance, the performance of ChatGPT for classifying the five personality and suicide ideation classifications was lower than the other pre-trained language models (e.g., BERT) [1]. The observations from prior studies indicate that ChatGPT is a generalist model that can perform many different text classification tasks without specialized training, yet dedicated training is required to achieve good results on specific tasks such as annotating contextualized online risk data.

Researchers have also explored the potential of LLM-based CAs as tools for identifying themes and grouping the textual data into identified themes (e.g., grounded thematic analysis) to reduce time and labor for such analysis [37]. For instance, Zhang et al. developed GPT-based data analysis tools to identify major themes in textual data and highlighted the potential of leveraging LLMs for augmenting efficiency in qualitative data analysis. As such, prior studies highlighted the potential benefits of the use of LLMs as AI-based tools to facilitate text annotation tasks. However, most of the prior work shed light on the potential of LLM-based CAs for text annotation tasks to alternate human labor for the same tasks; hence, leaving potential for co-labeling tasks with human coders under-explored. This gap is pertinent because co-labeling tasks need to support a two-way interactive discussion that can add nuance and context, and help generate a rationale for the various decisions, particularly in the context of online risk behavior, which is highly contextual in nature [3]. While modern conversational agents have shown the ability to interact with humans and work with examples [16, 19], their performance in collaborative text annotation exercises where different facets of co-labeling are important is as yet understudied. Here, we consider LLMs-based CAs as potentially useful co-labeling agents, which could support high-quality text annotations with explanations. Particularly, we situate this discussion in the data annotation of online risks.

Leveraging Large Language Models (LLMs) to Support Collaborative Human-Al Online Risk Data Annotation 1 2024, May 12, 2024, Honolulu, HI, USA

The concept of online risk is highly subjective and nuanced, and contextual sensitivity should be considered when identifying online risk [17]. For instance, oftentimes, social media users use sarcasm or even more creative ways to get around content moderation [33]. This phenomenon has become increasingly common in user-generated content on social media platforms [31]. Hence, newer ways to innovate and re-think labeling in such settings could have a significant methodological impact on HCI and social computing research. To address the issues of annotating subjective and subtle online risk data using LLM-based CAs, Huang et al. [13] experimented with the ChatGPT to annotate hate speech in tweets into three categories: implicit hate speech, non-hate speech, and uncertain. The results showed that ChatGPT correctly recognized implicit hate speech in 80% of the tweets with explanations better than those provided by human coders (i.e., crowdsourced annotators). The results from prior studies shed light on the potential of LLM-based CAs for text annotation tasks to alternate human labor for the same tasks. However, once again, it should be noted that the concept of risk and annotating online risk can be highly dependent on a variety of factors including cultural imprint, personality, political orientation, and contextual knowledge, hence, can lead to disagreement even among human coders. It is important that this insight does not lead to capitulation in the face of complexity but, instead, inspires better methods of automated analysis. Therefore, the combination of manual and automated content analysis is suggested as the gold standard for identifying online risk [6]. Here, we do not consider LLMs-based CAs as pretrained classifiers for text annotation but rather as potentially useful co-labeling agents, which under the right settings of frequent and nuanced interaction could support high-quality annotations with explanations. Such an approach if feasible and successful, could allow for scalability in content analysis. Further, this can open doors to understanding nuances that might be lost even by human coders, who also have limited world awareness and cognitive abilities.

3 DESIGN CONSIDERATIONS

We consider LLM-based CAs as promising co-annotation partners because they are systems enabled with the ability to interact with the users using natural human dialogue [30] have shown promising results in text annotation tasks due to their accuracy and adaptability (e.g., [1, 13, 15, 18, 36, 37]). The overarching question that we are interested in addressing is *"How can we design and implement a system that facilitates collaborative data annotation between researchers and conversational agents?"* We reflect on some of the potential challenges with the use of LLMs in contextualized and/or sensitive online risk data annotation tasks and provide design considerations for building LLMs-based research tools to effectively facilitate human-AI collaborative online risk data annotation.

- Interactivity: Interactivity is the heart of LLMs. Partially, interaction between humans and AI through LLMs helps alleviate one of the major issues inherent to AI-based systems, transparency. To this end, "How can we leverage interactive conversation between humans and AI to support highly nuanced contextualized online risk data annotation tasks at scale?"
- **Context-Awareness**: LLMs work by tokenizing the texts into words and processing them [23]. Therefore, how they understand risky interaction can differ from how humans do. The difference can be pertinent, especially for online risk data as risk is highly subjective and nuanced. Therefore, understanding how LLMs process textual data and make sense of information processed from textual data is a critical area for further exploration.
- **Prompt Design**: The responses generated by LLMs-based models are highly dependent on the prompts. Therefore, the quality of prompts could be the foundation for effective human-AI collaboration for data annotation tasks. Recently, various prompting tuning approaches have been proposed and examined to elicit responses that

are consistent and context-aware. Therefore, we ask "How can we design prompts that can best support highly nuanced and contextualized online risk data annotation tasks?"

- **Consistency**: LLMs are known to provide inconsistent responses even with the same prompts given for the same query, and the reasons why they generate inconsistent responses are still in a black box. One way to increase consistency is through well-designed prompts given for specific tasks. Another option might be to combine responses from multiple iterations to identify consistent trends in the output. The remaining question here is "How can we design LLMs workflows to generate online risk labels with high consistency?"
- User Interface: There are potential features to maximize the benefit of LLMs-based online risk data annotation tools by helping (e.g., features to feed interaction logs between researchers and AI into prompts). At the same time, a complex user interface with advanced features may increase the burden for researchers to train themselves to use the systems. Moreover, it can make the data annotation process lengthy and prone to errors. Therefore, a streamlined user interface while providing a set of features to support effective human-AI collaboration for online risk data annotation tasks is needed.
- Data Privacy and Security: When using LLMs to process online risk data, a primary concern for researchers is data privacy and security. For instance, OpenAI's policies explicitly stipulate that data submitted by users through their API will not be used to train their models [22]. Yet, we acknowledge that the conversation logs between researchers and AI can potentially be stored in the OpenAI API server for further usage. Therefore, researchers should also consider building LLM-based data annotation tools with private servers so that the training dataset is not shared via the web.

4 CONCLUSION

Our research interests align very well with the purposes of the LLMs as Research Tools workshop to identify ongoing applications and challenges of using LLMs to work with data in HCI research. We anticipate learning more about organizers' and participants' ground-breaking research ideas to reshape the HCI community's methods for working with data. In addition, participating in the workshop would be extremely beneficial for us to have a discourse on critical and ethical perspectives of the application of LLMs in HCI research. While we have identified some of the design condensations of LLM-based data annotation tools to support human-AI collaboration, we hope that participating in the workshop will help us address some of the remaining challenges and come up with additional design implications. Finally attending the workshop will be a valuable opportunity to interact with and gain insights from organizers and participants, which could potentially lead to future collaboration opportunities.

5 ABOUT THE AUTHORS

Jinkyung Park is a postdoctoral scholar in the Department of Computer Science at Vanderbilt University. Her research focuses on Human-Computer Interaction to promote online safety for youth and vulnerable populations.

Pamela Wisniewski is an associate professor in the Department of Computer Science at Vanderbilt University. Her work lies at the intersection of Human-Computer Interaction, Social Computing, and Privacy. Her expertise helps her empower end users and teach students to understand the value of user-centered design and evaluation.

Vivek Singh is an associate professor in the School of Communication and Information at Rutgers University. He designs AI systems that are responsive to human values and needs.

Leveraging Large Language Models (LLMs) to Support Collaborative Human-AI Online Risk Data Annotation 2024, May 12, 2024, Honolulu, HI, USA

REFERENCES

- Mostafa M Amin, Erik Cambria, and Björn W Schuller. 2023. Will Affective Computing Emerge From Foundation Models and General Artificial Intelligence? A First Evaluation of ChatGPT. *IEEE Intelligent Systems* 38, 2 (2023), 15–23.
- [2] Nată M Barbosa and Monchu Chen. 2019. Rehumanized crowdsourcing: A labeling framework addressing bias and ethics in machine learning. In Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems. 1–12.
- [3] Jody Clay-Warner. 2003. The context of sexual violence: Situational predictors of self-protective actions. Violence and victims 18, 5 (2003), 543-556.
- [4] Kevin Coe, Kate Kenski, and Stephen A Rains. 2014. Online and uncivil? Patterns and determinants of incivility in newspaper website comments. Journal of Communication 64, 4 (2014), 658–679.
- [5] Johannes Daxenberger, Marc Ziegele, Iryna Gurevych, and Oliver Quiring. 2018. Automatically detecting incivility in online discussions of news media. In 2018 IEEE 14th International Conference on e-Science (e-Science). IEEE, 318–319.
- [6] Katharina Esau. 2022. Content Analysis in the Research Field of Incivility and Hate Speech in Online Communication. In Standardisierte Inhaltsanalyse in der Kommunikationswissenschaft–Standardized Content Analysis in Communication Research: Ein Handbuch-A Handbook. Springer Fachmedien Wiesbaden Wiesbaden, 451–461.
- [7] R Stuart Geiger, Kevin Yu, Yanlai Yang, Mindy Dai, Jie Qiu, Rebekah Tang, and Jenny Huang. 2020. Garbage in, garbage out? Do machine learning application papers in social computing report where human-labeled training data comes from?. In Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency. 325–336.
- [8] Nir Grinberg, Kenneth Joseph, Lisa Friedland, Briony Swire-Thompson, and David Lazer. 2019. Fake news on Twitter during the 2016 US presidential election. Science 363, 6425 (2019), 374–378.
- [9] Soo-Hye Han, LeAnn M Brazeal, and Natalie Pennington. 2018. Is civility contagious? Examining the impact of modeling in online political discussions. Social Media+ Society 4, 3 (2018), 2056305118793404.
- [10] Benjamin D Horne, William Dron, Sara Khedr, and Sibel Adali. 2018. Assessing the news landscape: A multi-module toolkit for evaluating the credibility of news. In Companion Proceedings of the The Web Conference 2018. 235–238.
- [11] Homa Hosseinmardi, Sabrina Arredondo Mattson, Rahat Ibn Rafiq, Richard Han, Qin Lv, and Shivakant Mishra. 2015. Analyzing labeled cyberbullying incidents on the instagram social network. In International conference on social informatics. Springer, 49–66.
- [12] Mark Hsueh, Kumar Yogeeswaran, and Sanna Malinen. 2015. "Leave your comment below": Can biased online comments influence our own prejudicial attitudes and behaviors? Human communication research 41, 4 (2015), 557–576.
- [13] Fan Huang, Haewoon Kwak, and Jisun An. 2023. Is chatgpt better than human annotators? potential and limitations of chatgpt in explaining implicit hate speech. arXiv preprint arXiv:2302.07736 (2023).
- [14] Seunghyun Kim, Afsaneh Razi, Gianluca Stringhini, Pamela J Wisniewski, and Munmun De Choudhury. 2021. You Don't Know How I Feel: Insider-Outsider Perspective Gaps in Cyberbullying Risk Detection. In Proceedings of the International AAAI Conference on Web and Social Media, Vol. 15. 290–302.
- [15] Taja Kuzman, Igor Mozetic, and Nikola Ljubešic. 2023. Chatgpt: Beginning of an end of manual linguistic data annotation? use case of automatic genre identification. ArXiv, abs/2303.03953 (2023).
- [16] Vivian Lai, Samuel Carton, Rajat Bhatnagar, Q Vera Liao, Yunfeng Zhang, and Chenhao Tan. 2022. Human-ai collaboration via conditional delegation: A case study of content moderation. In Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems. 1–18.
- [17] Anna Litvinenko. 2023. The role of context in incivility research. In Challenges and perspectives of hate speech research, Christian Strippel, Sünje Paasch-Colberg, Martin Emmer, and Joachim Trebbe (Eds.). Digital Communication Research, Vol. 12. Berlin, 73–85. https://doi.org/10.48541/dcr.v12.5
- [18] Yiheng Liu, Tianle Han, Siyuan Ma, Jiayue Zhang, Yuanyuan Yang, Jiaming Tian, Hao He, Antong Li, Mengshen He, Zhengliang Liu, et al. 2023. Summary of ChatGPT-Related Research and Perspective Towards the Future of Large Language Models. *Meta-Radiology* (2023), 100017.
- [19] Maximilian Mackeprang, Claudia Müller-Birn, and Maximilian Timo Stauss. 2019. Discovering the sweet spot of human-computer configurations: A case study in information extraction. Proceedings of the ACM on Human-Computer Interaction 3, CSCW (2019), 1–30.
- [20] Michael Muller, Christine T Wolf, Josh Andres, Michael Desmond, Narendra Nath Joshi, Zahra Ashktorab, Aabhas Sharma, Kristina Brimijoin, Qian Pan, Evelyn Duesterwald, et al. 2021. Designing ground truth and the social life of labels. In Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems. 1–16.
- [21] OpenAI. 2023. Introducing ChatGPT. https://openai.com/blog/chatgpt
- [22] OpenAI. 2024. Security & Privacy. https://openai.com/security
- [23] OpenAI. 2024. What are tokens and how to count them? https://help.openai.com/en/articles/4936856-what-are-tokens-and-how-to-count-them
- [24] Kadir Bulut Ozler, Kate Kenski, Steve Rains, Yotam Shmargad, Kevin Coe, and Steven Bethard. 2020. Fine-tuning for multi-domain and multi-label uncivil language detection. In Proceedings of the Fourth Workshop on Online Abuse and Harms. 28–33.
- [25] Cliodhna O'Connor and Helene Joffe. 2020. Intercoder reliability in qualitative research: debates and practical guidelines. International journal of qualitative methods 19 (2020), 1609406919899220.
- [26] Jinkyung Park, Rahul Ellezhuthil, Ramanathan Arunachalam, Lauren Feldman, and Vivek Singh. 2022. Toward Fairness in Misinformation Detection Algorithms. In Workshop Proceedings of the 16th International AAAI Conference on Web and Social Media. Retrieved from https://doi.org/10.36190.

CCAI 2024, May 12, 2024, Honolulu, HI, USA

- [27] Jinkyung Park, Rahul Dev Ellezhuthil, Joseph Isaac, Christoph Mergerson, Lauren Feldman, and Vivek Singh. 2023. Misinformation Detection Algorithms and Fairness across Political Ideologies: The Impact of Article Level Labeling. In Proceedings of the 15th ACM Web Science Conference 2023. 107–116.
- [28] Jinkyung Park, Joshua Gracie, Ashwaq Alsoubai, Gianluca Stringhini, Vivek Singh, and Pamela Wisniewski. 2023. Towards Automated Detection of Risky Images Shared by Youth on Social Media. In Companion Proceedings of the ACM Web Conference 2023. 1348–1357.
- [29] Stephen A Rains, Kate Kenski, Kevin Coe, and Jake Harwood. 2017. Incivility and political identity on the Internet: Intergroup factors as predictors of incivility in discussions of news online. Journal of Computer-Mediated Communication 22, 4 (2017), 163–178.
- [30] Minjin Rheu, Ji Youn Shin, Wei Peng, and Jina Huh-Yoo. 2021. Systematic review: Trust-building factors and implications for conversational agent design. International Journal of Human–Computer Interaction 37, 1 (2021), 81–96.
- [31] Sergio Rojas-Galeano. 2017. On obstructing obscenity obfuscation. ACM Transactions on the Web (TWEB) 11, 2 (2017), 1-24.
- [32] Leonie Rösner and Nicole C Krämer. 2016. Verbal venting in the social web: Effects of anonymity and group norms on aggressive language use in online comments. Social Media+ Society 2, 3 (2016), 2056305116664220.
- [33] Farig Sadeque, Stephen Rains, Yotam Shmargad, Kate Kenski, Kevin Coe, and Steven Bethard. 2019. Incivility detection in online comments. In Proceedings of the eighth joint conference on lexical and computational semantics (* SEM 2019). 283–291.
- [34] Vivek K Singh, Souvick Ghosh, and Christin Jose. 2017. Toward multimodal cyberbullying detection. In Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems. 2090–2099.
- [35] Anke Stoll, Marc Ziegele, and Oliver Quiring. 2020. Detecting impoliteness and incivility in online discussions: Classification approaches for German user comments. Computational Communication Research 2, 1 (2020), 109–134.
- [36] Bowen Zhang, Daijun Ding, and Liwen Jing. 2022. How would stance detection techniques evolve after the launch of chatgpt? arXiv preprint arXiv:2212.14548 (2022).
- [37] He Zhang, Chuhao Wu, Jingyi Xie, ChanMin Kim, and John M Carroll. 2023. QualiGPT: GPT as an easy-to-use tool for qualitative coding. arXiv preprint arXiv:2310.07061 (2023).
- [38] Adam G Zimmerman and Gabriel J Ybarra. 2016. Online aggression: The influences of anonymity and social modeling. Psychology of Popular Media Culture 5, 2 (2016), 181.

6