August 2025

Far Enough to Share: Impact of Psychological Distance on GenAI Disclosure

Muriel Frank
Interdisciplinary Centre for Security, Reliability and Trust (SnT), muriel.frank@uni.lu

Ayah Tharwat
University of Luxembourg, ayah.tharwat@uni.lu

Nadia Pocher
University of Luxembourg, nadia.pocher@uni.lu

Far Enough to Share: Impact of Psychological Distance on GenAI Disclosure

Completed Research Full Paper

Muriel Frank
University of Luxembourg
muriel.frank@uni.lu

Ayah Tharwat
University of Luxembourg
ayah.tharwat@uni.lu

Nadia Pocher
University of Luxembourg
nadia.pocher@uni.lu

Abstract

Employees are increasingly using generative artificial intelligence (GenAI) tools to facilitate and automate work processes. While this may seem beneficial at first glance, employees are also prone to (un)consciously sharing sensitive information, putting organizations at risk. So far, we lack insight into what drives disclosure behavior with GenAI tools. Drawing on construal-level theory, this study examines how psychological distance influences such behavior. Our survey of more than 198 working GenAI users suggests that social proximity as well as spatial, temporal, and hypothetical distance positively affects disclosure behavior. Our findings not only contribute to the current literature on GenAI but also help practitioners to understand how employees share sensitive information with GenAI tools.

Keywords

Generative AI, Construal Level Theory, Psychological Distance, Disclosure Behavior, Privacy.

Introduction

The growing adoption of generative artificial intelligence (GenAI) tools, such as ChatGPT or Copilot, is swiftly reshaping how organizations and industries operate (van Dis et al., 2023). In the workplace, more and more employees rely on these tools to streamline processes, automate tasks, and increase productivity (Fui-Hoon Nah et al., 2023). Alongside the benefits, the heavy reliance on GenAI tools introduces several privacy risks, specifically concerning the disclosure of sensitive information (Zhou & Wu, 2024). A recent report involving 10,000 employees indicated that 15% have directly pasted work data into GenAI tools, specifically ChatGPT, and 6% have disclosed sensitive information . This improper disclosure increases the risk of data leakages, unauthorized access to sensitive data, and misuse, which can be detrimental to the organization (Huang et al., 2023). Of particular concern is that most users are unaware that any data they disclose could be used to train some GenAI tools, which can lead to privacy issues, copyright infringement, and information security vulnerabilities (Autio et al., 2024). According to recent reports by both the US Federal Trade Commission (FTC) and National Institute of Standards and Technology (NIST), traces of sensitive information were found within the data sets used to train the models, due to a process known as data memorization (Autio et al., 2024; FTC, 2023).

Currently, there is scant evidence on what drives GenAI disclosure behavior (Zhou & Wu, 2024), as patterns of disclosure vary depending on the use cases – e.g., Mireshghallah et al. (2024). For instance, disclosure levels differ between tasks like searching or language learning on ChatGPT and more sensitive tasks such as data analysis or drafting work emails (Zhang et al., 2024). Studies found that human-like chatbot interactions led to higher levels of information disclosure (Ischen et al., 2020), which provides precedent on why disclosure behavior to GenAI is deemed unique. Psychological distance, a concept from Trope and

Liberman's Construal Level Theory (Trope & Liberman, 2010), offers a promising lens for understanding this behavior. Psychological distance has been widely used in explaining online privacy behaviors (Hallam & Zanella, 2017) and has been shown to affect employees' security awareness and how they construe security incidents (Jaeger et al., 2017). Our study presents a novel use of CLT to explore the factors driving sensitive information disclosure when using GenAI tools. Our research question is as follows:

RQ: How does psychological distance affect information disclosure with GenAI tools?

To answer this research question, the present study builds upon Construal Level Theory (CLT) to better understand how users perceive the consequences of disclosure when using GenAI tools – here: ChatGPT – in a work context. CLT's focus on psychological distance provides insights into why users disclose sensitive information (Trope & Liberman, 2010), allowing for generalizable findings on GenAI behavior. To do so, we employ a scenario-based survey approach (Johnston et al., 2016) to examine how social proximity, as well as spatial, temporal, and hypothetical distance, affect disclosure. Our findings suggests that the psychological distance dimensions have a positive effect on sensitive information disclosure, thereby providing new insights into the influence of CLT on information security behavior. Understanding disclosure behavior and its antecedents can foster greater security awareness and bring users one step closer to shifting to a more security centric mindset (Bulgurcu et al., 2010).

To answer our research question, the paper is structured into five sections. The first section provides our theoretical foundation and background on GenAI, CLT and information disclosure, followed by of our research model and hypotheses. The second section introduces our methodology and data collection. The third section presents the data analysis and obtained results to verify our hypotheses. The fourth section outlines our research findings, theoretical contributions, and practical implications. Lastly, we discuss the limitations and present a synthesis of our overall study conclusions.

Theoretical Background and Hypotheses

Generative Artificial Intelligence

Generative Artificial Intelligence is a subset of AI that uses machine-learning models, including but not limited to large language models (LLM), which are trained on extensive amounts of data to generate text, images, or audio (Zhou & Wu, 2024). An important aspect of GenAI is its ability to memorize data from disclosed information that can later be regurgitated as a response (Hartmann et al., 2023). Although not all GenAI tools rely on memorization, LLMs such as ChatGPT are one of the prominent models that do so. While data memorization enhances response accuracy, if a model was trained on sensitive information, then outputs resulting from data memorization may generate privacy, security, and copyright issues (Hartmann et al., 2023). In this context, disclosure behavior is an important component to better understand the relationship that exists between GenAI tools and their users.

Research on the varying applications of ChatGPT and other GenAI tools is rapidly developing. Zhang et al. (2024) observed that most users were willing to trade-off their privacy to reap the benefits of GenAI – usefulness, convenience, tailored responses, etc. A preliminary study by Zhou and Wu (2024) explored the central (perceived affordance) and peripheral factors (privacy statement and privacy risk) on GenAI personal information disclosure. However, these studies have primarily investigated personal information disclosure and there exists a discrepancy between private and work-related contexts of disclosure behavior (Acquisti et al., 2012), which we seek to investigate for GenAI users.

Construal Level Theory and Psychological Distance

Construal level theory (CLT) is a framework connecting distance and abstraction. It suggests that psychological distance is an important determinant to measure how a person evaluates a situation. Psychological distance refers to one's subjective perception of how close or far he or she is from an object or event (Trope & Liberman, 2010). It is built on four dimensions of distance: (a) social—how similar or close the social target is to the perceiver's self (e.g. colleague/friend vs. stranger); (b) spatial—how physically distal the target is from the perceiver; (c) temporal—how much time (present vs. future) exists between the perceiver's present and the target event; and (d) hypothetical—how probable or realistic the target event seems as construed by the perceiver (Bar-Anan et al., 2006). Within the framework of psychological distance, as assumed through CLT, a perceiver will construe a target event as either a high-

level (abstract/distant) or low-level (concrete/near) construal (Trope et al., 2007). Since high-level construals are abstract representations of an event, the event appears more distant. By contrast, low-level construals are contextualized representations that include incidental features of an event, making the event seem more proximal (Trope et al., 2007). Psychological distance refers to the "when and where", while construal levels refer to the "why and how". Meaning that as construal levels increase, so does the perceived distance (Trope & Liberman, 2010).

The founders of CLT, Trope & Liberman (2003), have used psychological distance to explain and predict behaviors of perception, judgment, and decision making. Within the digital context, studies applying CLT have focused on consumer decision making for online shopping, and social networking sites (SNSs), concluding that there exists a correlational relationship between distance dimensions and consumer behavior – e.g., Darke et al. (2016). In an organizational and security context, Jaeger et al. (2017) found that when employees discern information security incidents as happening sooner rather than later, in their department instead of another company, to themselves or colleagues with similar characteristics instead of different employees, and as probable instead of unlikely, they are more aware of security threats and risks at work, and thus exhibit higher levels of information security awareness. Within the scope of our research, we apply CLT and psychological distance to measure the impact of the four distance dimensions on user disclosure behavior for GenAI interactions.

Information Disclosure

Information disclosure is the act of sharing personal or sensitive information. Sensitive information refers to data that requires confidentiality and discretion to safeguard against misuse or loss (Iannarelli & O'Shaughnessy, 2014). Information disclosure has been predominantly researched in contexts of SNSs, e-commerce, and mobile applications – e.g., Hallam & Zanella (2017). Most empirical studies on information disclosure have considered the cost-benefit analysis users make as an influencing factor of disclosure – e.g., Bandara et al., 2021). Additionally, that privacy concerns and trust in a company's security are key antecedents of online disclosure. They argue that the interrelation of these factors reduces the perceived risks of sharing sensitive information (Bandara et al., 2021; Metzger, 2004). Other factors such as social rewards and lack of privacy awareness have also contributed to the literature in understanding why people disclose personal or sensitive information when using platforms (Jiang et al., 2013). For GenAI disclosure, Zhang et al. (2024) observed that privacy-concerned users take steps like avoiding sensitive tasks on GenAI tools or sanitizing data before disclosure. While empirical research on GenAI disclosure is limited, we draw upon the existing literature and turn our attention towards examining the impact of psychological distance dimensions on ChatGPT disclosure behavior.

Hypotheses

Our study aims to examine the impact of psychological distance dimensions (social, spatial, temporal, hypothetical) on GenAI disclosure behavior, as illustrated in Figure 1. This model draws on the foundational framework of CLT by Trope & Liberman as it has been proven to aid in explaining online disclosure behavior – e.g., Darke et al. (2016). As the first study linking CLT to GenAI disclosure, we explore all four distance dimensions to establish their influence on the disclosure behavior of GenAI users in a work context.

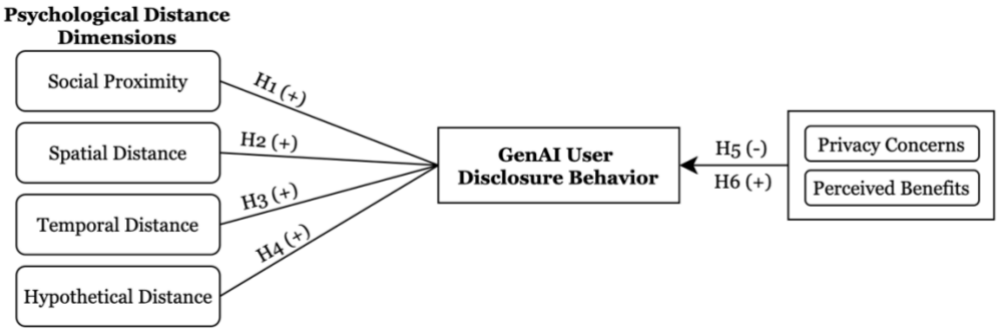

Figure 1. Research Model

As for privacy concerns, it has been extensively used to explain online sensitive information disclosure – e.g., Jiang et al (2013). Thus, we incorporate privacy concerns and perceived benefits as constructs within the context of GenAI to measure their influence on psychological distance, which in turn may influence disclosure behavior.

Embedded within social networks are relationships and interactions between individuals that play a fundamental role in spreading information and influencing behavior (Kim & Srivastava, 2007). Within the lens of psychological distance, social distance comparably affects decision making (Trope & Liberman, 2010). The closer and more trusted someone is at work, the more influential they will be on one's behavior – e.g., Kim & Srivastava (2007). For example, when employees hear about security incidents from close colleagues, they are more likely to be alert, compared to hearing it from distant colleagues (Jaeger et al., 2017). Applying these behavioral standards to GenAI disclosure, we postulate that the more socially distant someone is to oneself, the less influential they will be on one's disclosure behavior. Hence, our first hypothesis reads as follows:

H1: Social proximity will positively influence an individual's disclosure behavior

For our study, spatial proximity refers to how physically close a person is to an object or event. An object or event that is spatially distant is perceived as more abstract, broad, and far (Trope et al., 2007). For online behavior, a user will mentally construe physically distal risks as less threatening since they occur in a distal place (Bandara et al., 2017). This perception of distance alleviates the importance of security in a user's mind, thereby increasing the risks of them sharing sensitive information to GenAI. We expect that as the physical distance between the user and a potential risk increases, the less likely a user will behave securely. Thus, we hypothesize the following:

H2: Spatial distance will positively influence an individual's disclosure behavior.

Temporal distance refers to events happening in the future or ones that have occurred in the past (Trope & Liberman, 2010). Research has shown that individuals form more abstract representations, or high-level construals, of events happening in the distant-future over near-future events, which are construed more concretely (Trope & Liberman, 2003). In the context of information security, several authors used CLT and the temporal dimension to understand behavior. Studies found that temporal framing can be used to manipulate risk perceptions and behavioral intentions (Trope et al., 2007). When security incidents are framed as temporally close, people perceive the incident to be more concrete and likely to occur (Trope et al., 2007). This concrete representation evokes a higher sense of threat, thereby increasing alertness and information security awareness (Jaeger et al., 2017). Hence, we hypothesize the following:

H3: Temporal distance will positively influence an individual's disclosure behavior

When making decisions, people will evaluate the direct consequences and likelihoods associated. For negative consequences, certainty or likelihood exacerbates a risk or loss aversiveness, while uncertainty contributes to the attractiveness of a benefit or gain. The unlikelihood of an unwanted event occurring shifts a person's decision framing, thereby deviating from normative behavior (Tversky & Kahneman, 1981). According to CLT, hypotheticality has been correlated to decision making, as evidence showed that decreasing likelihood led individuals to represent events more abstractly. The more abstract an event is construed, the further it seems from the self (Bar-Anan et al., 2006). We thus hypothesize the following:

H4: Hypothetical distance will positively influence an individual's disclosure behavior

Some studies have suggested that privacy concerns are an antecedent of willingness to disclose information and are sought to increase reluctance towards sharing – e.g., Zhou & Wu (2024). Those with high levels of privacy concerns will employ different tactics to safeguard sensitive information and mitigate privacy-related risks (Son & Kim, 2008). Zhang et al. (2024) found that GenAI users with privacy concerns protected their data by: avoiding ChatGPT for sensitive tasks, sanitizing their data prior to sharing it, or providing fake information. We thus hypothesize the following:

H5: Privacy concerns will negatively influence an individual's disclosure behavior

People will tradeoff their privacy to accrue the benefits of an informational exchange. Previous research has confirmed that people are willing to share sensitive information online when the perceived benefits

outweigh the potential risks (Gieselmann & Sassenberg, 2023). Thus, we expect that the perceived benefits of GenAI such as usefulness, convenience, and tailored responses will play an influential role on sensitive information disclosure. We therefore hypothesize the following:

H6: Perceived benefits will positively influence an individual's disclosure behavior

Method

In this section, we present an overview of the study design and data collection procedure. We used a scenario-based survey approach which is well-established for capturing deviant behaviors in information security – e.g., Johnston et al. (2016). The survey was administered to 290 working professionals who utilize ChatGPT for work.

Survey Sample

Participants were approached through Prolific, a well-established platform for subject recruitment, to complete a 6-minute survey. The sample criteria were as follows: (1) employed in an organization (full-time or part-time), (2) use ChatGPT, (3) use AI tools at least once per week. A priori power analysis (GPower) determined a minimum required sample of 31 responses per scenario (Faul et al., 2007). Participants were excluded if they failed the attention (n=12) and realism checks (n=63), completed the survey significantly quickly (n=13), or exhibited biased responses (n=4). Thus, the final sample size consisted of 198 participants, mostly aged 25-44 (n=128), with a near-equal gender split (49.5% male, 50.5% female). The majority of participants were white (56%), held at least a bachelor's degree (78%), and had 3-9 years of work experience (42%).

Research Design

Using a scenario-based survey approach (Johnston et al., 2016), participants were asked to carefully read and respond to one of eight randomly assigned scenarios, with an attention check question in between to ensure validity. Each scenario described a situation in which Alex, a company employee, has a deadline at work and would like to utilize ChatGPT to help him finish a task that requires analysing sensitive data. Depending on the scenario, Alex is faced with a psychologically distant or proximal security incident that is disregarded in either case. Participants responded to a 7-point Likert scale measuring their likelihood of behaving similar to Alex (see Appendix A).

Measures and Validation

The survey comprised of 22 items, adapted from existing scales, found in Appendix B. All items and scenarios were measured on a 7-point Likert scale range, with 7 being 'strongly agree' and randomized for validity. A pretest (n=8) confirmed clarity and realism, leading to minor refinements. Additionally, the choice to predominantly focus on ChatGPT for this study was substantiated by the unanimous responses to the question e.g. "What GenAI tool do you use?", in which ChatGPT was indicated.

To empirically evaluate the impact of psychological distance on user disclosure behavior, we used a pre-validated scenario from Johnston et al. (2016) to construct all eight of our scenarios and grounded them in CLT. Three researchers developed and pretested the scenarios for realism and comprehensibility. Participants were asked to relay their agreement with Alex's. Realism questions shown in Appendix A were embedded to ensure participants could relate to the scenarios (Johnston et al., 2016). Those who did not perceive the scenario to be realistic (Likert average < 4) were excluded.

Participants were asked questions regarding privacy concerns and perceived benefits of ChatGPT. To measure privacy concerns, we adapted six items from Miltgen et al. (2016) that had a Cronbach's alpha of $\alpha = 0.906$. To evaluate the perceived benefits ($\alpha = 0.937$), we adapted a 4-item scale from Davis et al. (1989). Lastly, we controlled for age, gender, ethnicity, level of education, work experience, and weekly AI use.

Data Analysis and Results

To examine the influence of psychological distance on disclosure behavior, our analysis utilized a linear regression model in IBM SPSS. We tested models with 1) six control variables (age, gender, ethnicity, level of education, work experience, and weekly AI use) only to establish the extent of significance on psychological distance, 2) the main determinants: psychological distance dimensions as well as privacy concerns and perceived benefits. Ordinal regression confirmed our linear regression results. Key assumptions were met: Variance Inflation Factor (VIF) values were below 3.4, indicating no multicollinearity; multivariate normality was confirmed; and the Durbin-Watson statistic (1.87) suggested no autocorrelation. Out of eight dimensions, social proximity, spatial, temporal, and hypothetical distance were significant predictors (see Table 1).

Starting with H1, results showed that social proximity was a significant predictor of ChatGPT disclosure. H2 confirmed a positive relationship exists between spatial distance and risky behavior. In line with H3, our results indicate that temporal distance significantly influences disclosure behavior, suggesting that as the temporal distance between a user and a potential security incident increases, the incident is more likely to be perceived as less risky. Results for H4 demonstrated that when users perceive a security incident as highly unlikely, they will behave riskier or feel more comfortable disclosing sensitive information.

Variable	Direct Influence		
	β	Std. Error	p-value
Social Proximity→ Disclosure Behavior	0.305	0.626	0.011*
Social Distance→ Disclosure Behavior	0.156	0.573	0.163 n.s.
Spatial Proximity→ Disclosure Behavior	0.214	0.629	0.77 n.s.
Spatial Distance→ Disclosure Behavior	0.319	0.574	0.004**
Temporal Proximity→ Disclosure Behavior	0.224	0.625	0.058 n.s.
Temporal Distance→ Disclosure Behavior	0.446	0.619	<0.001***
Hypothetical Proximity→ Disclosure Behavior	0.136	0.595	0.213 n.s.
Hypothetical Distance→ Disclosure Behavior	0.414	0.625	<0.001***
Privacy Concerns→ Disclosure Behavior	-0.044	0.124	0.533 n.s.
Perceived Benefits→ Disclosure Behavior	-0.064	0.124	0.360 n.s.

*p <0.05; **p <0.01; ***p <0.001 ns: not significant

Table 1. Linear Regression Results

On the contrary, there was no statistically significant evidence that social distance, as well as spatial, temporal and hypothetical proximity influenced disclosure behavior. Both privacy concerns and perceived benefits, as well as the control variables were not statistically significant.

Discussion

Our study used a scenario-based approach to investigate and measure the influence of psychological distance dimensions on disclosure behavior of GenAI tools. Our results demonstrate that there exists a positive relationship between psychological distance and ChatGPT disclosure behavior.

Theoretical Contributions & Practical Implications

We grounded our research on Trope and Liberman's construal level theory and put forward a model to explain GenAI disclosure behavior along with potential factors impacting behavior. While CLT is a well-researched theory in behavioral information security and preliminary studies have used it to understand security and policy awareness – e.g., Jaeger et al. (2017) –, our study expands this application to an emerging technology, providing a novel dimensionality on how psychological distance dimensions influence the behavioral dynamics of GenAI users in the workplace.

In accordance with literature, our results show that social proximity, spatial, temporal, and hypothetical distance play varying roles on how much sensitive information users choose to share. A possible explanation for this may be tied to optimism bias in which people adopt a "won't happen to me" attitude, shifting the

responsibility of secure behavior onto others or the technology – GenAI (Owen et al., 2024). On the other hand, when people perceive information security incidents to be proximal, they have a desire to comply with those around them and with secure environments (Johnston et al., 2016).

One unanticipated result was that privacy concerns and perceived benefits did not significantly impact disclosure behavior. While our participants did not seem to significantly weigh the costs and benefits of disclosing sensitive data, our findings cannot be extrapolated to all GenAI users, as circumstance and threat levels may differ. This could be attributed to the notion that privacy perceptions differ depending on the user, security knowledge, and other factors (Metzger, 2004). Additionally, it could indicate that other underlying factors such as trust, normalization, or past disclosure could be drivers of ChatGPT information disclosure (Jaeger et al., 2017). Nonetheless, these important findings demonstrate the efficacy of using CLT and provide new insights into GenAI user behaviors within the work context of information security.

With the swift adoption and use of GenAI in organizations, it is important to address the practical implications of our work. Our findings highlight that employees do not shy away from using GenAI tools in the workplace and factors such as privacy concerns and perceived benefits have no positive effect on information disclosure. When employees perceive themselves to be psychologically distant from consequences, they tend to underestimate risks and assume negative outcomes are unlikely to affect them. Such detachment from responsibilities and abstraction of threats can lead to less secure behavior and greater vulnerability to malicious actors. Organizations must be aware that most GenAI users do not fully grasp how the technology works and how their data can be used maliciously (Autio et al., 2024). Hence, organizations must address this by enhancing and adapting usage policies and security awareness training around GenAI to minimize sensitive information disclosure among employees (Gieselmann & Sassenberg, 2023). By bridging the knowledge gap around how GenAI works and what is deemed "acceptable" versus "sensitive" to share, users can better safeguard their data and mitigate security risks in organizations.

Limitations and Future Research

The generalizability of our results is subject to certain limitations. While there are strengths to focusing on one information security-related problem within scenario-based surveys (Aurigemma & Mattson, 2019), our research model, though grounded in literature, is not exhaustive. Future work could extend this by examining trust, normalization, and security awareness levels as determinants or moderators of disclosure (Mireshghallah et al., 2024; Zhang et al., 2024). This would provide further insights into ChatGPT disclosure behavior and the filtering metrics ChatGPT users employ to identify what is acceptable data to share. Another limitation is the absence of manipulation checks. Future studies could incorporate them to validate whether participants perceived the intended psychological distance dimension. Lastly, the scenario items were self-reported, which is often criticized for introducing bias (Chan, 2009). Against this backdrop, a field study would be a natural progression of this work to more accurately grasp disclosure behavior.

Conclusion

Our study examines CLT's psychological distance dimensions on GenAI sensitive information disclosure. The results confirm that proximal relationships and distal information security incidents indeed reduce the risk levels of a threat, hence encouraging insecure behavior. This research contributes to the ongoing theoretical framework of CLT by applying it to an emerging technology. Given these results, organizations are presented with a synopsis of employee dynamics with GenAI tools that help them tailor policies and security training to increase awareness and promote secure behavior. Prior to this study, limited empirical research understood the behavioral dynamics involved in this emerging technology—GenAI. Our findings set the foundation for further exploration into GenAI information disclosure and its antecedents to enhance security and mitigate threat landscapes.

Acknowledgements

This work was funded by Luxembourg's National Research Fund (FNR) and PayPal – PEARL grant ref. 13342933/Gilbert Fridgen. For open access purposes, the authors have applied a CC BY 4.0 license to any Author Accepted Manuscript arising from this submission.

REFERENCES

Acquisti, A., John, L. K., & Loewenstein, G. (2012). The Impact of Relative Standards on the Propensity to Disclose. *Journal of Marketing Research*, *49*(2), 160–174. https://doi.org/10.1509/jmr.09.0215

Aurigemma, S., & Mattson, T. (2019). Generally Speaking, Context Matters: Making the Case for a Change from Universal to Particular ISP Research. *Journal of the Association for Information Systems*, 1700–1742. https://doi.org/10.17705/1jais.00583

Autio, C., Dunietz, J., Hall, P., Jain, S., Roberts, K., Schwartz, R., Stanley, M., & Tabassi, E. (2024, July). *Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile*. National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.600-1.pdf

Bandara, R. J., Fernando, M., & Akter, S. (2017). The Privacy Paradox in the Data-Driven Marketplace: The Role of Knowledge Deficiency and Psychological Distance. *Procedia Computer Science*, *121*, 562–567. https://doi.org/10.1016/j.procs.2017.11.074

Bandara, R. J., Fernando, M., & Akter, S. (2021). Construing online consumers' information privacy decisions: The impact of psychological distance. *Information & Management*, *58*(7), 103497. https://doi.org/10.1016/j.im.2021.103497

Bar-Anan, Y., Liberman, N., & Trope, Y. (2006). The association between psychological distance and construal level: Evidence from an implicit association test. *Journal of Experimental Psychology: General*, *135*(4), 609–622. https://doi.org/10.1037/0096-3445.135.4.609

Bulgurcu, Cavusoglu, & Benbasat. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quarterly*, *34*(3), 523. https://doi.org/10.2307/25750690

Chan, D. (2009). So why ask me? Are self report data really that bad? In C. E. Lance & R. J. Vandenberg (Eds.), *Statistical and methodological myths and urban legends: Doctrine, verity and fable in the organizational and social sciences* (pp. 309–335). Routledge.

Darke, P. R., Brady, M. K., Benedicktus, R. L., & Wilson, A. E. (2016). Feeling Close From Afar: The Role of Psychological Distance in Offsetting Distrust in Unfamiliar Online Retailers. *Journal of Retailing*, *92*(3), 287–299. https://doi.org/10.1016/j.jretai.2016.02.001

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User Acceptance of Computer Technology: A Comparison of Two Theoretical Models. *Management Science*, *35*(8), 982–1003. https://doi.org/10.1287/mnsc.35.8.982

Faul, F., Erdfelder, E., Lang, A.-G., & Buchner, A. (2007). G*Power 3: A flexible statistical power analysis program for the social, behavioral, and biomedical sciences. *Behavior Research Methods*, *39*(2), 175–191. https://doi.org/10.3758/BF03193146

FTC. (2023). *FTC file no. 232-3044, civil investigative demand schedule*. Federal Trade Commission. https://www.washingtonpost.com/documents/67a7081c-c770-4f05-a39e-9d02117e50e8.pdf

Fui-Hoon Nah, F., Zheng, R., Cai, J., Siau, K., & Chen, L. (2023). Generative AI and ChatGPT: Applications, challenges, and AI-human collaboration. *Journal of Information Technology Case and Application Research*, *25*(3), 277–304. https://doi.org/10.1080/15228053.2023.2233814

Gieselmann, M., & Sassenberg, K. (2023). The More Competent, the Better? The Effects of Perceived Competencies on Disclosure Towards Conversational Artificial Intelligence. *Social Science Computer Review*, *41*(6), 2342–2363. https://doi.org/10.1177/08944393221142787

Hallam, C., & Zanella, G. (2017). Online self-disclosure: The privacy paradox explained as a temporally discounted balance between concerns and rewards. *Computers in Human Behavior*, *68*, 217–227. https://doi.org/10.1016/j.chb.2016.11.033

Hartmann, V., Suri, A., Bindschaedler, V., Evans, D., Tople, S., & West, R. (2023). *SoK: Memorization in General-Purpose Large Language Models* (arXiv:2310.18362). arXiv. http://arxiv.org/abs/2310.18362

Huang, K., Zhang, F., Li, Y., Wright, S., Kidambi, V., & Manral, V. (2023). Security and Privacy Concerns in ChatGPT. In K. Huang, Y. Wang, F. Zhu, X. Chen, & C. Xing (Eds.), *Beyond AI: ChatGPT, Web3, and the Business Landscape of Tomorrow* (pp. 297–328). Springer. https://doi.org/10.1007/978-3-031-45282-6_11

Iannarelli, J. G., & O'Shaughnessy, M. (2014). *Information Governance and Security: Protecting and Managing Your Company's Proprietary Information*. Butterworth-Heinemann.

Ischen, C., Araujo, T., Voorveld, H., Van Noort, G., & Smit, E. (2020). Privacy Concerns in Chatbot Interactions. In A. Følstad, T. Araujo, S. Papadopoulos, E. L.-C. Law, O.-C. Granmo, E. Luger, & P. B. Brandtzaeg (Eds.), *Chatbot Research and Design* (Vol. 11970, pp. 34–48). Springer International Publishing. https://doi.org/10.1007/978-3-030-39540-7_3

Jaeger, L., Ament, C., & Eckhardt, A. (2017). The Closer You Get the More Aware You Become – A Case Study about Psychological Distance to Information Security Incidents. *ICIS 2017 Proceedings*.

Jiang, Z. (Jack), Heng, C. S., & Choi, B. C. F. (2013). Research Note—Privacy Concerns and Privacy-Protective Behavior in Synchronous Online Social Interactions. *Information Systems Research*, *24*(3), 579–595. https://doi.org/10.1287/isre.1120.0441

Johnston, A. C., Warkentin, M., McBride, M., & Carter, L. (2016). Dispositional and situational factors: Influences on information security policy violations. *European Journal of Information Systems*, *25*(3), 231–251. https://doi.org/10.1057/ejis.2015.15

Kim, Y. A., & Srivastava, J. (2007). Impact of social influence in e-commerce decision making. *Proceedings of the Ninth International Conference on Electronic Commerce*, 293–302. https://doi.org/10.1145/1282100.1282157

Metzger, M. J. (2004). Privacy, Trust, and Disclosure: Exploring Barriers to Electronic Commerce. *Journal of Computer-Mediated Communication*, *9*(4). https://doi.org/10.1111/j.1083-6101.2004.tb00292.x

Miltgen, C. L., Henseler, J., Gelhard, C., & Popovič, A. (2016). Introducing new products that affect consumer privacy: A mediation model. *Journal of Business Research*, *69*(10), 4659–4666. https://doi.org/10.1016/j.jbusres.2016.04.015

Mireshghallah, N., Antoniak, M., More, Y., Choi, Y., & Farnadi, G. (2024). *Trust No Bot: Discovering Personal Disclosures in Human-LLM Conversations in the Wild*. http://arxiv.org/abs/2407.11438

Owen, M., Flowerday, S. V., & Van Der Schyff, K. (2024). Optimism bias in susceptibility to phishing attacks: An empirical study. *Information & Computer Security*. https://doi.org/10.1108/ICS-02-2023-0023

Son & Kim. (2008). Internet Users' Information Privacy-Protective Responses: A Taxonomy and a Nomological Model. *MIS Quarterly*, *32*(3), 503. https://doi.org/10.2307/25148854

Trope, Y., & Liberman, N. (2003). Temporal construal. *Psychological Review*, *110*(3), 403–421. https://doi.org/10.1037/0033-295X.110.3.403

Trope, Y., & Liberman, N. (2010). Construal-Level Theory of Psychological Distance. *Psychological Review*, *117*(2), 440–463. https://doi.org/10.1037/a0018963

Trope, Y., Liberman, N., & Wakslak, C. (2007). Construal Levels and Psychological Distance: Effects on Representation, Prediction, Evaluation, and Behavior. *Journal of Consumer Psychology*, *17*(2), 83–95. https://doi.org/10.1016/S1057-7408(07)70013-X

Tversky, A., & Kahneman, D. (1981). The Framing of Decisions and the Psychology of Choice. *Science*, *211*(4481), 453–458. https://doi.org/10.1126/science.7455683

van Dis, E. A. M., Bollen, J., Zuidema, W., van Rooij, R., & Bockting, C. L. (2023). ChatGPT: Five priorities for research. *Nature*, *614*(7947), 224–226. https://doi.org/10.1038/d41586-023-00288-7

Zhang, Z., Jia, M., Lee, H.-P. (Hank), Yao, B., Das, S., Lerner, A., Wang, D., & Li, T. (2024). "It's a Fair Game", or Is It? Examining How Users Navigate Disclosure Risks and Benefits When Using LLM-Based Conversational Agents. *Proceedings of the CHI Conference on Human Factors in Computing Systems*, 1–26. https://doi.org/10.1145/3613904.3642385

Zhou, T., & Wu, X. (2024). Examining generative AI user disclosure intention: An ELM perspective. *Universal Access in the Information Society*. https://doi.org/10.1007/s10209-024-01130-1

Appendix A

Scenario A[1]: Hypothetical Distance

Alex has a deadline at work and wants to use ChatGPT to help him finish a task that requires analyzing sensitive work data. He knows the company requires employees to anonymize sensitive data if they use ChatGPT for work. Alex has done so for previous tasks and understands the importance of protecting the client's sensitive data from potential ChatGPT vulnerabilities. He has a deadline soon and knows that with ChatGPT he can finish the task on time, but anonymizing the data will take too much time and effort. Alex believes that the information he discloses will not be compromised, but if it were, there is a **high likelihood** a privacy risk would occur. Regardless, he decides to use ChatGPT to complete the task.

Please select an answer for the following items as they relate to the scenario.

	SD[2]						*SA[3]*
In this situation, I would do the same as Alex	1	2	3	4	5	6	7
Anonymizing data takes too much time and effort	1	2	3	4	5	6	7
The above scenario is a realistic one	1	2	3	4	5	6	7
If I were Alex, I would have also disregarded the likely risk	1	2	3	4	5	6	7
I could imagine a similar scenario taking place at work	1	2	3	4	5	6	7
I think I would do what Alex did if this happened to me	1	2	3	4	5	6	7
The situation could occur at work	1	2	3	4	5	6	7

[1]Scenarios available upon request; [2]SD=Strongly disagree; [3]SA=Strongly agree

Appendix B

Construct	Item		Source
Privacy concerns	PC1	I am concerned that information I disclose to ChatGPT is shared with third parties	Miltgen et al. (2016)
	PC2	I am concerned that my interactions with ChatGPT are monitored/tracked	
	PC3	I believe information that I disclose to ChatGPT is at risk	
	PC4	I am concerned that ChatGPT stores my information without my permission	
Perceived Benefits	PB1	ChatGPT improves my performance at work	Davis et al. (1989)
	PB2	ChatGPT increases my productivity at work	
	PB3	ChatGPT helps me accomplish work tasks quicker	
	PB4	Overall, I find GenAI to be a useful and effective tool	