Navigating privacy concerns in the age of large language models: The roles of AI Literacy and critical thinking

Student Name: Loïs Schoemaker
Student Number: 625815

Supervisor: Vivian Chen

Master Media studies – Media & Business
Erasmus School of History, Culture and Communication
Erasmus University Rotterdam

Master's Thesis
June 23rd, 2024

Word Count: 15121 words

Navigating privacy concerns in the age of large language models: The roles of AI Literacy and critical thinking

ABSTRACT

The increasing use of large language models (LLMs) has gotten significant attention due to their advanced capabilities in natural language processing, helping with different tasks such as text generation, translation, and summarization. The use of this AI technology differs from educational to professional settings. However, researchers have voiced their concerns about their potential to generate biased outputs, compromise information privacy, and misuse sensitive data.

Privacy concerns are crucial in understanding user interactions with LLMs. The IUIPC model by Malhotra et al. (2004) has been extensively used to study privacy concerns and their impact on risk beliefs, primarily in internet usage contexts. Attitude is another common consequence of privacy concerns frequently studied together with risk beliefs. This study applied the IUIPC model to LLMs to explore these relationships further. The study identified a gap in exploring how AI literacy moderates and critical thinking mediates the relationship between privacy concerns, risk beliefs and attitudes toward LLMs. AI literacy encompasses understanding AI capabilities, limitations, and ethical considerations, which is crucial for responsible use of LLMs. This research aims to fill these gaps by examining these moderating and mediating effects using a quantitative survey, providing insights into privacy concerns in the context of LLMs.

The findings from this study indicate that privacy concerns influence both risk beliefs and attitudes toward LLMs. Privacy concerns positively impact risk beliefs, suggesting that individuals with higher privacy concerns perceive greater risks when using LLMs. However, privacy concerns have a weak negative correlation with attitudes toward LLMs, though this relationship was not statistically significant. Critical thinking was found to partially mediate the relationship between privacy concerns and attitude but did not mediate the relationship between privacy concerns and risk beliefs. Additionally, AI literacy was tested as a moderator, but only two out of the three subscales, critical appraisal and practical application, significantly moderated the relationship between privacy concerns and attitudes, managing the negative impact of privacy concerns on attitudes toward LLMs. Technical understanding did not significantly moderate the relationship between privacy concerns and attitude. None of the subscales of AI literacy moderated the relationship between privacy concerns and risk beliefs.

KEYWORDS: *Privacy concerns, risk beliefs, attitude, AI literacy, critical thinking, large language models.*

Table of Contents

1. Introduction

Over the past few years, Artificial Intelligence (AI) technologies have witnessed substantial progress across multiple domains (Marr, 2023, p. 1). These AI technologies can improve the daily lives of individuals in a number of areas, including healthcare, transportation, customer service, and education (Kelly et al., 2023, p. 2). Predictions suggest that these technologies will progress even more in the coming years as AI will impact most industries and contribute an estimated US $15.7 trillion to the worldwide economy by 2030 (Murphy et al., 2021, p. 2). As this technology revolution is taking place, there is a growing interest in researching AI and its impact and consequences. This research will dive deeper into an emerging field of study in the context of AI; large language models (LLMs).

1.1. The rise of large language models

The most famous and recent LLM is ChatGPT (Marr, 2023. p. 1). The impressive capabilities of LLMs, such as ChatGPT, have provoked a range of responses from people and researchers all over the world as this AI development seems to bring about a substantial change in the way that people interact with and utilize AI technology (Jo & Park, 2024, p. 2). LLMs can provide many potential benefits, such as quick and efficient access to domain-specific information, assistance with literature review, text generation support, language translation, and automated summarization (Lund & Wang, 2023, p. 27). Studies have shown that assignments made by ChatGPT obtain higher grades than those made by students (Vázquez-Cano et al., 2023, p. 5). Observations of this nature do not escape the attention of students, who are inclined to utilize the tool (Raman et al., 2023, p. 5; Rueda et al., 2023, p. 2). Not only do students use this tool, but statistics show that employees are inclined to experiment with the tool in their work environment as well (Petrosyan, 2024, p. 1).

With the rise of LLMs in various settings, there is a growing need to investigate the dynamics surrounding the new technology. It is important to ensure that the use of the technology is ethical and free of unwanted plagiarism (Perkins, 2023, p. 14). However, research has shown that there are multiple privacy issues with using LLMs, such as ChatGPT (Wu et al., 2023). According to Lund and Wang (2023) the outputs may be biased because they may reflect the biases in the training data. This might lead to unfair or erroneous findings that negatively impact disadvantaged groups. Furthermore, it has the potential to produce sensitive data that needs to be secured and not disclosed without approval, such as financial, medical, and personal information. Additionally, it can produce impersonating text, which might deceive or impersonate someone else, infringing on their information privacy. For example, in the context of students, this means students' information privacy can be compromised when they submit their academic work to LLMs, such as ChatGPT, for comments or grading, as there exists a potential for the model to retain and distribute the content or personal information without proper authorization (Lund & Wang, 2023, p. 28).

Information privacy is defined as “an individual's claim to control the terms under which personal information – information identifiable with the individual – is acquired, disclosed, and used” (Privacy Working Group, 1997, as cited in Kim et al., 2023, p. 1). Furthermore, it entails the capacity to create, oversee, and implement regulations for handling personal information within group and social settings (James & Bélanger, 2020, p. 510). In this context, privacy concerns about personal information are one of the foremost problems during this technological revolution in the digital age (Kim et al., 2023, p. 1). This research will focus on this definition of privacy concerns.

1.2. Privacy concerns: risk beliefs and attitude

In the literature, privacy concerns are associated with several consequences. A recent meta-analysis on privacy concerns by Kim et al. (2023) categorized the consequences into three different groups: behavioral intentions, behavior, and cognitive appraisals. Cognitive appraisals of privacy concerns are perceived risk and attitude. Existing studies focusing on the effects of privacy concerns and its consequences have used the Internet Users’ Information Privacy Concerns (IUIPC) model by Malhotra et al. (2004) to examine privacy concerns and risk perceptions. The existing studies focus on these relationships in the broader contexts of Internet usage, such as e-commerce or social media platforms (Dinev et al., 2008; Fortes et al., 2017; Kim et al., 2023; Malhotra et al., 2004). However, there is a notable gap in the literature regarding the application of this model to understand the effect of privacy concerns on risk perceptions and attitude in the context of LLMs. Therefore, this research will use the IUIPC model to study the relationship between privacy concerns, perceived risk, and attitude in the context of LLM users. Attitude as a variable is not included in the IUIPC model, but is frequently studied as a consequence of privacy concerns together with risk beliefs (Kim et al, 2023, p. 3), so it is added to the research model of this study using the AI Attitude scale by Grassini (2023).

Additionally, while there is active research on risk beliefs, and attitude toward AI and the relationships between trust and privacy concerns on the adoption of AI (Ashoori & Weisz, 2019; Bitkina et al., 2020; Hasan et al., 2021; Kelly et al., 2023), there remain inconsistencies in the findings of the relationship among behavioral intentions and the behavior that is grounded in privacy concern (Brough & Martin, 2020; Pitardi & Marriott, 2021). This is called the privacy paradox (Norberg et al., 2007, p. 101). Although people claim they cherish their privacy and are concerned about data protection, they frequently reveal more information than they mean to when asked for personal information. People's decisions about providing personal information can be influenced by various factors, including perceived risks related to data sharing and trust in the organization requesting the information. Despite privacy concerns, people may be more willing to provide information to trustworthy companies (Norberg et al., 2007, p. 106-107).

1.3. Research gap and relevance

Since there are multiple privacy issues with using LLMs, such as ChatGPT (Wu et al., 2023), AI literacy is crucial for enabling people to critically evaluate and responsibly utilize large language models, particularly in the context of privacy concerns, ethical considerations, and e.g. the potential impact on academic integrity (Perkins, 2023, p. 10). AI literacy encompasses understanding the capabilities, limitations, and ethical considerations of AI (Ng et al., 2021 p. 2). It is argued that AI literacy is crucial for people to live, work, and learn in the current digital world through AI-driven technologies (Steinbauer et al., 2021, p. 131). The specific role of AI literacy in moderating the relationship between privacy concerns and its effect on risk perceptions and attitude in the context of LLMs is not yet explored. There is limited discussion on how AI literacy influences people's perceptions of risk and attitude when using LLMs. Existing studies focus on broader aspects of AI literacy and how people must learn about AI from an early age (Lee et al., 2021; Su et al., 2023) without delving into its specific implications for people engaging with LLMs and the effect on their risk beliefs and attitude in relation to their privacy concerns.

Additionally, in research on privacy concerns and its consequences, among other suggestions by Kokolakis (2017) cognitive abilities have not yet been carefully researched from an empirical standpoint to explain the privacy paradox (Kokolakis, 2017, p. 132). A subset of cognitive abilities is computational thinking. Computational thinking skills encompass creativity, cooperativity, algorithmic thinking, problem-solving, and critical thinking (ISTE & CSTA, 2011). Previous research has showed that computational thinking is highlighted as a significant determinant of AI literacy (Çelik, 2023, p. 7). Considering the role of computational thinking in enhancing AI literacy, people with higher levels of critical thinking skills, which are part of computational thinking, may be better equipped to understand and evaluate the implications of privacy concerns in AI technologies (Çelik, 2023, p. 5).

Therefore, this research will fill the gaps in the literature by introducing AI literacy as a potential moderator and critical thinking as a potential mediator to research how individuals' critical thinking skills and AI literacy influence the relationship between privacy concerns, risk beliefs, and attitude towards LLMs. By applying the IUIPC model in the context of LLMs and considering the influence of AI literacy and critical thinking, this study seeks to provide insights into the unique dynamics shaping people's attitudes towards privacy and trust in AI-driven environments. This is particularly relevant given the growing use of LLMs in various fields (Rueda et al., 2023, p. 2; Petrosyan, 2024). The research question guiding this investigation is:

"To what extent do AI literacy moderate and critical thinking mediate the relationship between privacy concerns and the perceived risk and attitude of large language model users?"

The purpose of the study is to fill the gaps in the literature and add to the academic discourse on privacy concerns with new technologies, such as LLMs, and their consequences. The research attempts to present empirical data, gathered through a survey, on how AI literacy and critical thinking affect people's feelings of risk and attitude when utilizing LLMs. By understanding the moderating role of AI literacy and the mediating role of critical thinking, policymakers can establish policies and educational initiatives that enable people to navigate privacy concerns and make well-informed choices about the use of LLMs. Additionally, the research findings can help and inform AI developers in creating LLMs with transparent algorithms and improved privacy features. Developers can encourage the responsible and ethical use of AI technologies in various settings by addressing privacy concerns and fostering trust. Furthermore, understanding the impact of AI literacy and critical thinking on risk beliefs and attitude can directly benefit people by creating a better-informed environment. By equipping people with the necessary knowledge and skills to critically evaluate AI technologies, they can make informed choices that protect their privacy.

In summary, answering this research question can be relevant for educational institutions, work environments, AI developers, students, educators, and AI policymakers, as the results can help inform the development of guidelines, educational programs, and technological solutions to address how AI literacy and critical thinking can inform privacy related challenges associated with using LLMs.

2. Theoretical framework

To address the research gap, a theoretical framework is essential to guide the investigation. In this chapter, the theoretical concepts related to the research question are presented by defining AI, LLMs, privacy concerns, risk beliefs, attitude, critical thinking and AI literacy. Additionally, an analysis of the IUIPC model by Matlhora et al. (2004) is presented. The hypotheses are proposed based on the findings in previous research related to the concepts of the research question. Finally, a conceptual model is presented addressing the scope of the study.

2.1. Large Language Models

This research focuses on individuals who use LLMs to help them in any type of way. LLMs are a subset of AI that specifically focuses on natural language processing (NLP) (Baidoo-Anu & Ansah, 2023, p. 53). There is no exact definition of AI, however, the European Commission defined AI after an overview of different definitions as "systems that display intelligent behavior by analyzing their environment and taking action – with some degree of autonomy – to achieve specific goals" (Samoili et al., 2020, p. 9). LLMs refer to advanced AI systems that are trained on massive amounts of text data to understand and generate human language. These models have a vast number of parameters, enabling them to process and generate human-like text with high accuracy and complexity (Tamkin et al., 2021, p. 2). The most popular LLMs, such as OpenAI's GPT (Generative Pre-trained Transformer) series and Google's BERT (Bidirectional Encoder Representations from Transformers), have hundreds of millions to billions of parameters. These models are typically pre-trained on vast amounts of text data from the internet, allowing them to learn the complex patterns and nuances of language. People can access these models online and utilize them for quick and efficient access to domain-specific information, assistance with literature review, text generation support, language translation, and automated summarization (Lund & Wang, 2023, p. 27).

Despite many benefits of using LLMs, there are several personal information privacy issues with LLMs (Pan et al., 2020, p. 1). It can potentially produce sensitive data that needs to be secured and not disclosed without approval, such as financial, medical, and personal information. Additionally, it can produce impersonating text, which might deceive or impersonate someone else, infringing on people's information privacy. For example, in the context of students, this means students' privacy can be compromised when they submit their academic work to LLMs, such as ChatGPT, for comments or grading, as there exists a potential for the model to retain and distribute the content without proper authorization (Lund & Wang, 2023, p. 28). Building on this, this study will look into people's privacy concerns who have used LLMs and the consequences that follow from these concerns.

2.2. IUIPC model

Privacy concerns indicate how someone feels about their personal data. Disclosing sensitive personal data is a privacy risk to individuals with a high privacy concern (Zhou, 2011, p. 213).

Addressing privacy concerns and perceived risks associated with AI technologies is essential for fostering consumer trust and encouraging adoption. Consumers often worry about the privacy risks linked to sharing personal information with AI systems. The complexity of AI and the potential for data misuse strengthen these concerns. By effectively addressing privacy issues and reducing risk beliefs, organizations can build trust, enhance user confidence, and increase the adoption of AI-driven products and services (Hasan et al., 2021, p. 592). A research model looking into people's information privacy concerns and their risk beliefs is the Internet Users' Information Privacy Concerns (IUIPC) model by Malhotra et al. (2004).

In the past, multiple scales were developed to measure privacy concerns. Building on the Concern for Information Privacy (CFIP) scale by Smith et al. (1996), which was designed to measure privacy concerns in various offline and online contexts, Malhotra et al. (2004) created the Internet Users' Information Privacy Concerns (IUIPC) scale, which specifically focuses on the online context, which makes it relevant for the context of LLMs as these are usually available online. This scale based on this model has three dimensions regarding privacy concerns: awareness of privacy practices, control, and collection. The dimension 'awareness of privacy practices' describes worries about communication and transparency around the use of personal data. Control refers to worries about being able to manage and alter personal information kept in databases. Lastly, collection relates to worries about the different types of personal information that online businesses acquire. Furthermore, risk beliefs are measured in the IUIPC scale in 4 items (Malhotra et al., 2004, p. 352).

The IUIPC model predicts that privacy concerns impact individuals' trust and risk beliefs, affecting their intentions to share personal information online. Specifically, higher privacy concerns lead to lower trusting beliefs and higher risk beliefs, reducing the intention of disclosing personal information. This model proposes that enhancing privacy awareness, reducing the amount of data collected, and increasing control over personal data can reduce privacy concerns, as a consequence trust will be improved and risk beliefs will be reduced (Malhotra et al., 2004, p. 347). Overall, the IUIPC model provides a strong framework for researching and assessing LLMs user's information privacy concerns and their risk beliefs, offering valuable insights into this critical aspect of online behavior and decision-making. This research enriches the discussion surrounding the IUIPC model by extending its application to the domain of AI technology, specifically LLMs, and incorporating AI literacy as a moderator and critical thinking as a mediator.

2.3. Risk beliefs and privacy concerns

A cognitive appraisal consequence of privacy concerns is perceived risk (Kim et al., 2023, p. 3). According to Malhotra et al. (2004), risk beliefs are defined as the expectation that there is a substantial chance of loss when providing personal information to (online) businesses (Malhotra et al., 2004, p. 341). The model suggests that Internet users' information privacy concerns have a positive effect on risk beliefs (Malhotra et al., 2004, p. 341). This relationship is based on the idea that

individuals who are more concerned about their information privacy are more cautious about the potential risks involved in sharing their personal data. Therefore, privacy concerns positively influence risk beliefs, indicating a stronger perception of risk associated with disclosing personal information online (Kim et al., 2023, p. 3). The research of Brough and Martin (2020) has confirmed that there is a relationship between privacy concerns and risk beliefs in institutions or organizations handling personal data. Individuals with heightened privacy concerns are more likely to perceive greater risks associated with online activities. This heightened perception of privacy risks can lead to increased caution in online behaviors as individuals strive to protect their personal information. Those individuals are more skeptical about sharing their information with entities they do not trust (Brough & Martin, 2020, p. 12).

Additionally, more research has shown that information privacy concerns are positively associated with risk beliefs (Gurung & Raja, 2016; Kim et al., 2023; Koohang et al., 2018; Xu et al., 2011). Xu et al. (2011) researched the relationship between information privacy concerns and perceived risk within the context of organizational information practices and institutional privacy assurances. Perceived risk is a specific aspect of individuals' risk beliefs that focuses on their subjective evaluation of the risks associated with sharing personal information online (Xu et al., 2011, p. 1), which is similar to the IUIPC model its risk beliefs (Malhotra et al., 2004, p. 341). The study found that perceived risk is a significant factor that contributes to individuals' privacy concerns, and it is interconnected with other elements such as privacy control, value of privacy, and institutional privacy assurances in shaping individuals' attitudes towards information privacy (Xu et al., 2011, p. 810). Furthermore, Gurung and Raja (2016) studied the relationship between privacy and risk beliefs in the context of online consumers and found there was a positive relationship. Internet users with high privacy concerns are high on risk beliefs (Gurung & Raja, 2016, p. 361).

In contrast to other findings Koohang et al. (2018), who studied privacy concerns and risk beliefs using the IUIPC model in the context of social media users, found that only collection, a subscale of privacy concerns, was positively associated with risk beliefs. Awareness of privacy practices and control, other subscales of privacy concerns, were insignificant related to risk beliefs (Koohang et al., 2018, p. 1219). This could be explained by several factors, such as the complexity of privacy policies, perceived control, normalization of risk, trust in platforms, and individual differences in risk perception (Koohang et al., 2018, p. 1221).

However, the privacy concern meta-analysis by Kim et al. (2023), which included 181 studies, concluded that overall privacy concerns were positively associated with risk beliefs. Therefore, based on the previous findings in the literature, I argue the following hypotheses:

H1: Privacy concerns are positively associated with the risk beliefs of users towards large language models.

2.4. Attitude and privacy concerns

Another cognitive appraisal consequence of privacy concerns is attitude (Kim et al., 2023, p. 3). Attitude reflects the psychological preference to assess a specific entity with varying degrees of approval or disapproval (Eagly and Chaiken, 1998, p. 269). Within the context of this research, people's attitude towards AI, LLMS specifically, is measured. The relationship between attitude and privacy concerns is based on the idea that people who are high on privacy concerns have negative attitudes toward information systems, in this case LLMs, because of the uncertainty surrounding the collection, storage, and use of personal data (Ketelaar & Van Balen, 2018, p. 178). Grassini (2023) developed the AI attitude scale to assess public attitudes towards AI based on 4-items validated in the study (Grassini, 2023, p. 9).

Previous studies have shown that privacy concerns are negatively associated with attitudes towards different technologies (Ketelaar & Van Balen, 2018; Kim et al., 2023; Park et al., 2021; Pitardi & Marriott, 2021). In the context of technology, Ketelaar and Van Balen (2018) found that people had more negative attitudes towards phone tracking when people were higher in privacy concerns (Keterlaar & Van Balen, 2018, p. 178). Similarly, in the context of AI technology, Pitardi and Marriott (2021) have found that privacy concerns had a negative impact on people's attitudes towards AI technology, specifically AI voice assistants. The study explained the negative impact of privacy concerns on users' attitudes toward voice-based artificial intelligence assistants by highlighting the understanding that individuals may have reservations about engaging with these technologies if they perceive potential risks to their privacy and data security (Pitardi & Marriott, 2021, p. 635). Similarly, Park et al. (2021) have found the same relationship between privacy concerns and attitude in the context of AI service robots (Park et al., 2021, p. 700). Additionally, Kim et al. (2023) concluded that privacy concerns were negatively associated with attitude following their meta-analysis on privacy concerns (Kim et al., 2023, p. 11). Therefore, based on the previous findings in the literature, I argue the following hypotheses:

H2: Privacy concerns are negatively associated with users' attitude toward large language models.

2.5. AI Literacy as a moderator

AI literacy is defined as understanding the capabilities, limitations, and ethical considerations of AI (Ng et al., 2021, p. 2). LLMs require a high level of AI literacy to understand and use the technology responsibly, as there are multiple privacy issues with using LLMs (Lund & Wang, 2023, p. 28; Wu et al., 2023). This research adapts the antecedents 'technical understanding', 'critical appraisal', and 'practical application' to measure AI literacy of the work of Laupichler et al. (2023) which has been developed and used to measure the AI literacy of non-experts in AI. The use of all

three antecedents for measuring AI literacy demonstrates a thorough method of evaluating the understanding and skills of individuals with AI technology.

The ‘technical understanding’ component of AI literacy is essential for recognizing the capabilities and limitations of LLMs, including their potential to generate biased, inaccurate, or even harmful content. People with high technical understanding are conscious of the complex ways AI works and is programmed, from recommendation engines and virtual assistants to driverless cars and medical diagnostics. By measuring technical understanding, the researcher can determine how well-informed people are regarding AI and the technicalities behind it (Laupichler et al., 2023, p. 6).

Additionally, the capacity to critically assess and examine AI data is known as ‘critical appraisal’. This entails evaluating the credibility, reliability, and biases of predictions, algorithms, and information produced by AI. People who are skilled at critical appraisal are able to differentiate between factual and false information, detect possible biases in AI systems, and recognize ethical considerations. The critical appraisal aspect of AI literacy is crucial for evaluating the trustworthiness and reliability of the outputs generated by LLMs, especially when used for tasks like research, writing, or decision-making. Assessing critical appraisal abilities offers perceptions of an individual’s ability to make well-informed choices on AI technology. Without adequate AI literacy, individuals may not be able to critically evaluate the data collection, processing, and usage practices of AI applications, leading to potential privacy violations and loss of control over personal information (Laupichler et al., 2023, p. 6).

Lastly, the capacity of a person to apply their knowledge and comprehension of AI ideas in practical settings is evaluated through ‘practical application’. This entails applying AI technologies to successfully solve issues, make choices, or complete tasks. AI technology may be used by people with strong practical application abilities to boost productivity, creativity, and innovation in a variety of fields, including business, education, healthcare, and entertainment. Assessing individuals' practical application abilities offers valuable information about their ability to use AI as a tool for decision-making and problem-solving. Practical application can empower individuals to utilize privacy-preserving techniques and tools when interacting with AI-powered services, such as managing data-sharing permissions. Furthermore, this dimension of AI literacy can help individuals navigate the appropriate use of LLMs, such as understanding the privacy implications of inputting personal information into these models and the potential for misuse or unintended consequences (Laupichler et al., 2023, p. 6).

These antecedents are consistent with the complex character of AI literacy, which includes not only the acquisition of information but also the critical thinking and practical application abilities necessary for understanding the complicated dynamics of the AI environment (Laupichler et al., 2023, p. 6).

In other words, higher AI literacy among users is linked with a more comprehensive understanding of the workings of LLMs and for example, the privacy protection mechanisms that are

put in place. This can play a significant role in shaping attitudes and risk beliefs towards AI technologies (Holmes et al., 2022, p. 40), as AI literacy is found to be significantly associated with attitudes towards using AI (Chai et al., 2020; Ng et al., 2021). Previous research has shown that users of LLMs, such as ChatGPT, generally have positive attitudes towards the technology (Bernabei et al., 2023; Tiwari et al., 2023). However, previous research by Yuan et al. (2023) showed that when people do not have enough knowledge to understand the AI mechanisms, which refers to AI literacy, individuals attribute biases to algorithms, people who programmed the AI, the company that implemented the AI, or themselves, which in turn results in more risk beliefs in AI (Yuan et al., 2023, p. 11). Therefore, individuals with higher AI literacy are likely to have a better understanding of the privacy implications of AI technologies, which may lead to lower privacy concerns and therefore lead to lower risk beliefs and positive attitudes. Thus, it is plausible to assume that users with lower AI literacy have a stronger association with risk and privacy concerns, along with a more negative attitude. This could stem from their heightened privacy-related worries as a result of an insufficient level of complete understanding. Therefore, AI literacy is proposed as a moderator on the relationship between privacy concerns and the risk beliefs and attitudes of users towards LLMs, as it can influence the strength or direction of the relationship between privacy concerns and its consequences risk beliefs, and attitudes. Therefore, implementing the subscales of AI literacy according to Laupichler et al. (2023) the following hypotheses are formed:

H3: The positive relationship between privacy concerns and the risk beliefs of people using large language models is weaker for users who score higher on technical understanding of AI.

H4: The positive relationship between privacy concerns and the risk beliefs of people using large language models is weaker for users who score higher on critical appraisal of AI.

H5: The positive relationship between privacy concerns and the risk beliefs of people using large language models is weaker for users who score higher on practical application AI.

H6: The negative relationship between privacy concerns and the attitude of people using large language models is weaker for users who score higher on technical understanding of AI.

H7: The negative relationship between privacy concerns and the attitude of people using large language models is weaker for users who score higher higher critical appraisal of AI.

H8: The negative relationship between privacy concerns and the attitude of people using large language models is weaker for users who score higher on practical application of AI.

2.6. Critical thinking as a mediator

In research on the relationship between privacy concerns and its consequences, Kokolakis (2017) has called for more careful empirical research on cognitive abilities (Kokolakis, 2017, p. 132). Cognitive abilities are defined as "aspects of mental functioning, such as memorizing and remembering; inhibiting and focusing attention; speed of information processing; and spatial and causal reasoning" (Robinson, 2012, p. 17). Previous research by Sun et al. (2024) has linked cognitive abilities to privacy concerns. The study showed that individuals with higher cognitive abilities process privacy-related information more effectively, leading to better comprehension of privacy policies and potential risks associated with data sharing. This can influence their decision-making regarding privacy disclosures. Additionally, cognitive abilities were associated with how individuals perceive and evaluate risks related to privacy. People with higher cognitive abilities are better at assessing the potential consequences of privacy disclosures and making informed decisions based on perceived risks, leading to more informed and rational decisions regarding data sharing. This implies higher cognitive abilities may enable individuals to better understand the implications of data sharing and the importance of privacy protection (Sun et al., 2024, p. 11).

Other research has linked cognitive abilities to privacy concerns in a different context, namely social media (Ahmed & Lee, 2023, p. 1). The study found that cognitive abilities can influence how individuals perceive and manage privacy risks in digital environments. People with high cognitive abilities are probably better able to evaluate the social media landscape and manage their privacy, which allows them to utilize social media more freely for a wider range of online activities. However, those with lower cognitive abilities can experience information overload on social media, which leads to higher concerns about online privacy. (Ahmed & Lee, 2023, p. 10).

It is acknowledged that an essential cognitive ability for the twenty-first century is computational thinking. It requires a variety of abilities and mental processes that are essential to information processing and problem-solving (ah et al., 2014, p. 1). Computational thinking skills encompass creativity, cooperativity, algorithmic thinking, problem-solving, and critical thinking (ISTE & CSTA, 2011). Critical thinking, characterized by the ability to analyze, evaluate, and synthesize information (Halpern, 2014, p. 8), serves as a cognitive lens in this research through which individuals perceive and respond to privacy-related challenges in their interactions with emerging technologies, particularly large language models.

Critical thinking is measured using the Computational Thinking Scales (CTS) by Korkmaz et al. (2017), a measurement tool that assesses various aspects of computational thinking skills. In particular, this study focusses on the factor of critical thinking within the scale. It is measured in 5 items (Korkmaz et al., 2017, p. 565).

Additionally, previous research has showed that computational thinking is highlighted as a significant determinant of AI literacy (Çelik, 2023, p. 7). Considering the role of computational thinking in enhancing AI literacy, people with higher levels of critical thinking skills, which are part

of computational thinking, may be better equipped to understand and evaluate the implications of privacy concerns in AI technologies (Çelik, 2023, p. 5). Therefore, critical thinking is introduced as a mediator in the relationship between privacy concerns and its consequences. This suggests that critical thinking serves as an intermediary process by which privacy concerns impact individuals' perceptions and responses, especially concerning their risk beliefs and their attitudes toward LLMs. The following results are hypothesized:

H9: Critical thinking will mediate the positive relationship between privacy concerns and the risk beliefs of people using large language models.

H10: Critical thinking will mediate the negative relationship between privacy concerns and the attitude of people using large language models.

2.7. Conceptual framework

The conceptual framework illustrated in the following figure is constructed based on the discussed concepts and the hypotheses that followed. It encompasses the four primary factors; privacy concerns, risk beliefs, and attitude, along with the introduced moderators AI literacy, and the mediator critical thinking.

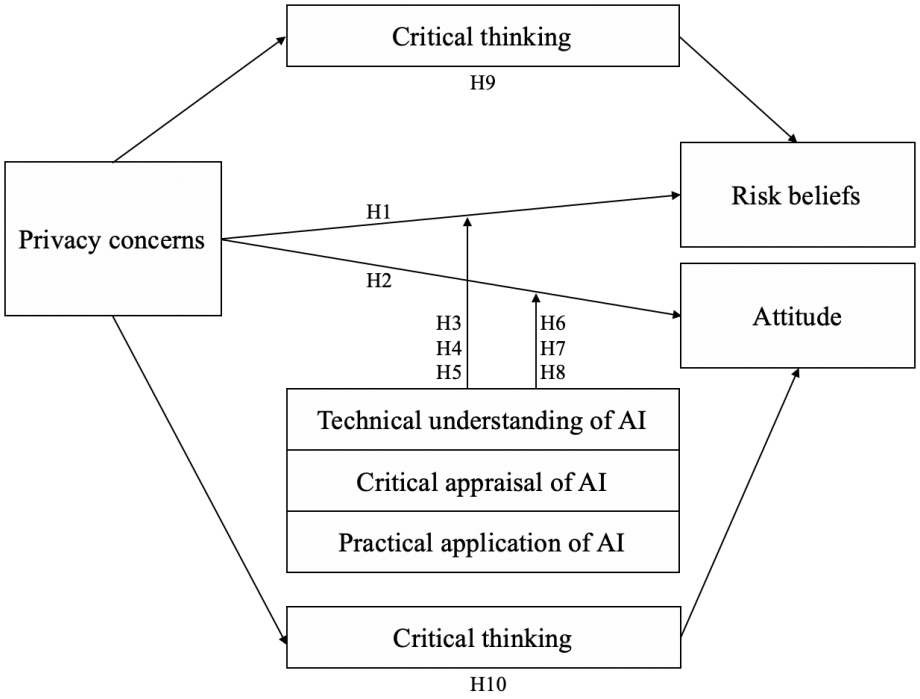

Figure 1: Conceptual framework

3. Method

This chapter provides a detailed explanation of the methodology, operationalization, and data analysis selection used to test the hypotheses based on the constructed conceptual model in the theoretical framework section. Finally, an explanation and justification are given for the validity and reliability of this study.

This research used a quantitative research method to answer the research question. Qualitative research focuses on gaining an in-depth understanding of experiences, motivations, and human behavior and relies on non-numerical data gained through interviews, focus groups, and observations. The goal of qualitative research methods is to explore the "why" and provide rich, contextual insights (Babbie, 2016, p. 24). In contrast, quantitative research focuses on collecting and analyzing numerical data to understand causal relationships, test hypotheses, and draw general conclusions. It typically involves experiments, surveys, and statistical analysis (Babbie, 2016, p. 25). The objective of this research is to test and verify the relationships among the variables of the conceptual model in the theoretical framework section, which makes this a quantitative study.

The quantitative research in this thesis involves data which was collected through the use of an online survey. The choice to use an online survey is motivated as the current study is focused on the correlations between different factors, such as privacy concerns and its cognitive appraisals, and the underlying processes that moderate these interactions, such as AI literacy and critical thinking. This decision was influenced by a survey's ability to enable the use of statistical analysis to examine the presence, direction, and size of effects related to the dependent and independent variables of interest (Babbie, 2016, p. 261). A survey is a suitable quantitative method for the gathering and analysis of extensive data from a sizable participant pool, thereby aiding in the recognition of patterns (Oates, 2005, p. 93). A quantitative survey will provide objective measures of people's privacy concerns, risk beliefs, attitudes, critical thinking, and AI literacy as they will be measured using validated scales. The online survey was made in Qualtrics.

3.1. Sampling

The target population of this research is people who have used LLMs. Participants had to have used a LLM at least once in their life to address their privacy concerns using the model and their risk beliefs and attitudes towards LLMs and AI. Additionally, participants had to be 18 years or older to participate in this research.

Due to time constraints, the sampling method that was used for this research was convenience sampling. This entails that respondents were selected from the part of the target population, who were easy to reach for the researcher because of their convenience accessibility (Taherdoost, 2016, p. 22). Additionally, convenience sampling allows for a quick and straightforward recruitment process, enabling the researcher to gather sufficient data for analysis within the constraints of the research resources and timeline. The researcher was able to attain a larger sample size outside of the limits of

the individual network by using the snowball approach (a sort of convenience sampling) of the online survey distribution, and by sharing the survey on LinkedIn and Facebook groups where people participate in each other's surveys or survey sharing websites such as SurveyCircle.com. Participants were requested to complete the survey by sharing the link with others on social media networks and platforms such as Whatsapp and LinkedIn.

3.2. Sample

In total, 269 answers were collected. The data collection took place from the 25th of April until the 16th of May. After completing the data collection, the data set was cleaned by eliminating all incomplete answers. Additionally, to ensure that participants had used large language models before, two control questions regarding their use were asked at the beginning of the survey. Given the length of the survey, many participants did not complete the study until the end. In the end, a sample of 155 answers was left for further analysis ($N = 155$). All of the 155 respondents accepted the informed consent form and stated that they were 18 years or older. All participants answered the survey in English.

Out of the 155 participants, 56 (36.1%) were male, 94 (60.6%) were female, 2 participants (1.3%) identified as 'Other' and 1 participant (0.6%) preferred not to say. The remaining 2 participants (1.3%) were missing. The participants' age ranged from 18 to 69, the most mentioned age was 24 ($Mo_{age} = 24$) and the average age was 28.53 ($SD = 10.54$).

The educational level of the participants was high, as the majority had a bachelor's degree (50.3%) or a master's degree (33.5%). Most participants were either enrolled as students (56.1%) or employed full-time (31.6%). Regarding the participants' nationalities, it can be said that most of the people were Dutch (76.8%). However, this survey reached people from other European countries such as Germany, Greece, Belgium, and Poland, as well as outside of Europe namely, America and Vietnam.

Participants had to be LLM users. Most people revealed that they use LLMs several times a week (28.4%), followed by once a month (21.3%), several times a month (19.4%), and even several times a day (18.1%). The remaining 20 participants (12.8%) were divided into once a week (5.2%), once a day (3.2%), several times an hour (2.6%), and all the time (1.9%).

3.3. Survey procedure

Before participating in the survey, participants were informed about the nature of the survey. This information included that the research was about their privacy concerns in LLMs, the survey duration and that participating in the research was voluntary. Additionally, participants were informed that all data would be anonymously collected and used for academic purposes only. If participants stated they were 18 years or older and agreed to the terms, they continued with the start of the survey. If participants did not agree with the terms mentioned, they were redirected to the end of the survey.

Participants that agreed first filled in questions about their LLM use followed by questions regarding their privacy concerns, their risk beliefs, their AI literacy, attitude towards AI and critical thinking skills. The final part of the survey addressed demographical questions about their age, gender identification, level of education, current occupation and nationality. The survey encompassed a total of 61 questions and typically took approximately 10 minutes to complete. The complete survey can be found in Appendix 1.

3.4. Operationalization

Several measurements assessed the effect of privacy concerns on risk beliefs, attitude, and the moderating effect of AI literacy and mediating effect of critical thinking, which is the main purpose of this research. This section will discuss measurements and operationalization of dimensions developed in the conceptual model such as demographics, privacy concerns, risk beliefs, attitude, critical thinking, and AI literacy. All the items of the listed dimensions were merged into one survey and tailored in Qualtrics. The scales were all previously validated and were accompanied by a seven-point Likert response scale which included 1; strongly agree, 2; agree, 3; somewhat agree, 4; neither agree or disagree, 5; somewhat disagree, 6; disagree, and 7; strongly disagree, allowing participants to express their agreement or disagreement with each statement.

3.4.1. Privacy concerns

The IUIPC scale of Malhotra et al. (2004) was used to measure privacy concerns. This scale has three dimensions regarding privacy: awareness of privacy practices, control, and collection. The questions were slightly adjusted to fit the purpose of this research. An example of this is "Companies seeking information online should disclose the way the data are collected, processed, and used" (Malhotra et al., 2004, p. 351) was changed to "Large language models seeking information online should disclose the way the data are collected, processed, and used". The dimension 'awareness of privacy practices' describes worries about communication and transparency around the use of personal data and consists of 3 items, including "It is very important to me that I am aware and knowledgeable about how my personal information will be used" (Malhotra et al., 2004, p. 351). Control refers to worries about being able to manage and alter personal information kept in databases. It consists of 3 items, including "Consumer online privacy is really a matter of consumers' right to exercise control and autonomy over decisions about how their information is collected, used, and shared" (Malhotra et al., 2004, p. 351). Lastly, collection relates to worries about the different types of personal information that online businesses acquire. It is measured in 4 items, including "It usually bothers me when large language model companies ask me for personal information". In the original article, composite reliability (CR) was reported instead of Cronbach's alpha. CR is often used in the context of confirmatory factor analysis (CFA) because it provides a more accurate estimate of reliability by considering the factor loadings and error variances of the items. The outcomes of Cronbach's alpha

and CR can be similar, but they will not always be exactly the same. CR values of .70 and higher are considered acceptable for research purposes, with higher values indicating better reliability and consistency of the scale items. (Peterson & Kim, 2013, p. 194).

In the original study, the CR values for the different dimensions of privacy concerns were as follows: Collection: CR = .83, Control: CR = .78, Awareness: CR = .74, Overall IUIPC scale: CR = .89. These CR values indicate the internal consistency reliability of the constructs, with values above .70 generally considered acceptable for reliability. The CR values suggest that the items within each dimension and the overall IUIPC scale are reliable measures of the constructs they represent. These values indicate a high internal consistency reliability for each dimension and for the overall IUIPC scale, suggesting that the items within each dimension and the scale as a whole effectively measure the intended constructs (Malhotra et al., 2004, p. 345). All items were tested on a 7-point Likert scale from 'strongly agree' to 'strongly disagree', similar to the original study.

Given that the original IUIPC scale measuring privacy concerns was adapted to focus on LLMs, the adjustments could alter the factor structure. Therefore, a principal component analysis (PCA) and reliability analysis was conducted on the modified scales. Conducting PCA ensures that the modified scale still reliably measures the same constructs as intended.

The 10 items for measuring privacy concerns which were Likert-scale based were entered into a confirmatory factor analysis using Principal Components extraction with Direct Oblimin rotation and number of factors was set as 3, $KMO = .83$, χ^2 ($N = 155, 45$) = 697.35, $p < .001$. The resultant model explained 70.1% of the variance in privacy concerns. Factor loadings of individual items onto the three factors found are presented in Table 1.

Table 1. Factor loadings, explained variance and reliability of the 3 factors found for the scale "privacy concerns".

Item	Control	Collection	Awareness
Consumer control of personal information lies at the heart of consumer privacy.	.88		
I believe that online privacy is invaded when control is lost or unwillingly reduced as a result of a marketing transaction.	.81		
Consumer online privacy is really a matter of consumers' right to exercise control and autonomy over decisions about how their information is collected, used, and shared.	.61		
It bothers me to give personal information to a large language model company.		-.95	
It usually bothers me when large language model companies ask me for personal information.		-.86	

When large language model companies ask me for personal information, I sometimes think twice before providing it.		-.83	
I'm concerned that large language models are collecting too much personal information about me.		-.78	
Large language models seeking information online should disclose the way the data are collected, processed, and used.			.92
A good consumer online privacy policy should have a clear and conspicuous disclosure.			.73
It is very important to me that I am aware and knowledgeable about how my personal information will be used.			.51
R^2	.44	.18	.08
Cronbach's α	.75	.88	.71

The PCA results confirm that the modified privacy concerns scale is multidimensional, with three distinct factors explaining 70.1% of the variance. The factors identified provide a comprehensive understanding of privacy concerns in the context of LLMs, with acceptable reliability as indicated by Cronbach's alpha values above .70 for all factors. The Cronbach's alpha for privacy concerns as one variable is .85, indicating that the subscales combined are stronger in reliability.

3.4.2. Risk beliefs

Risk beliefs were measured using the validated IUIPC scale, which measures it in 4 items (Malhotra et al., 2004, p. 352). The participants read a situation where they could get a free membership on a large language model website if they filled out a list regarding personal information and answer the questions regarding their risk beliefs. The items were adjusted to fit the purpose of the study. An example of this is "In general, it would be risky to give the information to online companies" (Malhotra et al., 2004, p. 352) was changed to "In general, it would be risky to give the information to large language model companies". The CR value of Risk beliefs in the original study indicates high internal consistency reliability; CR = .78 (Malhotra et al., 2004, p. 345). All items were tested based on a 7-point Likert scale from 'strongly agree' to 'strongly disagree', similar to the original study.

The reliability analysis for risk beliefs in this study showed that Cronbach's alpha was .89, indicating good internal consistency in the items in this study. Deleting any items would not increase reliability.

3.4.3. Attitude

Attitude was measured using the validated AI Attitude Scale (AIAS-4) by Grassini (2023). The AIAS-4 is a short self-report instrument that provides a quick and reliable measure of public attitudes toward AI in 4 items. It is designed to be easy to administer for researchers interested in understanding users' or citizens' attitudes toward AI. The scale's items are structured to capture a balanced assessment of attitudes toward AI, focusing on perceived utility, potential impact on society and humanity, and intentions to use AI technologies. The items were adjusted to fit the purpose of the study. This means that instead of attitudes towards AI, attitudes towards LLMs were tested. An example of this is “I believe that AI will improve my life” (Grassini, 2023, p. 7) was changed to “I believe that large language models will improve my life”. The Cronbach's alpha value for the original AIAS-4 scale was high (Cronbach’s α = .83). Cronbach’s alpha indicates the internal consistency reliability of the constructs, with values above .70 generally considered acceptable for reliability. This indicates that the internal consistency reliability of the scale is high (Grassini, 2023, p. 5). The original study uses a 10-point Likert scale to measure respondents’ attitudes. However, to keep the survey consistent with other scales, a 7-point Likert scale from ‘strongly agree’ to ‘strongly disagree’ was adopted. Research has shown that 5-, 7-, and 10-point scales are similar in terms of data characteristics such as variance, skewness, and kurtosis. This means that researchers have flexibility in selecting any scale format without significantly impacting the analytical tools employed in marketing research (Dawes, 2008, p. 9).

To ensure that the measured constructs are reliable, a reliability analysis was conducted. During the reliability analysis of the Attitude AIAS-4 scale, it was observed that the item “I think large language model technology is a threat to humans,” which was a reversed item and recoded before analysis, significantly reduced the overall reliability of the scale. The initial Cronbach's alpha for the 4-item scale was .70. Deleting this item would improve the scale's internal consistency (Cronbach’s α = .85).

Additionally, the AIAS-4 scale measuring attitude towards AI was adapted to focus on large language models. These adjustments could potentially alter the factor structure. Therefore, a principal component analysis (PCA) was conducted on the modified scales. Conducting PCA ensures that the modified scale still reliably measures the same constructs as intended.

The original 4 items measuring attitude which were Likert-scale based were also entered into a confirmatory factor analysis using Principal Components extraction with Direct Oblimin rotation and the number of factors was set as 1. Initially, all items were included in the analysis to determine their suitability for the scale, KMO = .70, χ^2 (N = 155, 6) = 223.60, p < .001. The resultant model explained 59.5% of the variance in attitudes toward large language models. However, similar to the reliability analysis, one item ("I think large language model technology is a threat to humans") was found to have a low communalities value and did not load well on the primary factor. Removing this item increased

Cronbach's alpha, indicating improved reliability. Factor loadings of individual items onto the factor found are presented in Table 3.

Then a factor analysis with the remaining 3 items was conducted and showed increased scores, $KMO = .71$, χ^2 ($N = 155, 6$) = 212.92, $p < .001$. The resultant model explained 77.5% of the variance in attitudes toward large language models. Factor loadings of individual items onto the factor found are presented in Table 3.

Table 2. Factor loadings, explained variance and reliability of the original "attitude" scaleas measured in the survey.

Item	Attitude
I believe that large language models will improve my work.	.90
I think I will use large language model technology in the future.	.86
I believe that large language models will improve my life.	.86
I think large language model technology is a threat to humans	.30
R^2	.60
Cronbach's α	.70

Table 3. Factor loadings, explained variance and reliability of the final "Attitude" scale as used for analysis.

Item	Attitude
I believe that large language models will improve my work.	.92
I think I will use large language model technology in the future.	.88
I believe that large language models will improve my life.	.85
R^2	.77
Cronbach's α	.85

The PCA and reliability analysis confirm that the modified attitude scale, after deleting one item, is unidimensional and reliably measures positive attitudes toward LLMs. The deletion of one item was necessary to enhance the internal consistency of the scale, as proven by the increase in Cronbach's alpha from .70 to .85. This process ensures that the scale accurately reflects the construct it is designed to measure.

3.4.4. AI literacy

AI literacy is be measured using the validated Scale for the Assessment of Non-Experts in AI (SNAIL). It consists of 31 items that measure three factors: technical understanding, critical appraisal, and practical application (Laupichler et al., 2023, p. 7). The SNAIL scale aims to evaluate individuals' understanding of AI concepts, their ability to critically assess AI applications, and their practical knowledge of applying AI in various contexts. Technical understanding assesses individuals' knowledge and comprehension of AI concepts, technologies, and applications. It focuses on understanding the technical aspects of AI, such as how AI algorithms work, the capabilities of AI systems, and the general principles behind artificial intelligence. It consists of 14 items, including "I can describe how machine learning models are trained, validated and tested" (Laupichler et al., 2023, p. 7). Cronbach's alpha showed excellent reliability for this subscale (Cronbach's α = .93). Critical appraisal evaluates individuals' ability to evaluate AI applications and results critically. It involves assessing the strengths and limitations of AI technologies, understanding ethical considerations related to AI use, and being able to analyze the impact of AI on various aspects of society. It is measured in 10 items, including "I can explain why data privacy must be considered when developing and using artificial intelligence applications" (Laupichler et al., 2023, p. 7). Cronbach's alpha also showed excellent reliability for this subscale (Cronbach's α = .91). Lastly, practical application measures individuals' practical knowledge and skills in applying AI in real-world scenarios. It includes understanding how AI can be used in different contexts, identifying suitable AI solutions for specific problems, and being able to effectively utilize AI tools in practical situations. It is measured in 7 items, including "I can give examples from my daily life (personal or professional) where I might be in contact with artificial intelligence" (Laupichler et al., 2023, p. 7).). Lastly, Cronbach's alpha also showed excellent reliability for this subscale *(*Cronbach's α = .85). This means the internal consistency of the three scales in the three-factor model in the original study is excellent (Laupichler et al., 2023, p. 5). All items were tested based on a 7-point Likert scale from 'strongly agree' to 'strongly disagree', similar to the original study.

To ensure that the measured constructs in this study are reliable, a reliability analysis was conducted. The analysis showed that the subscales technical understanding *(*Cronbach's α = .95), critical appraisal *(*Cronbach's α = .92), and practical application *(*Cronbach's α = .88), indicating good internal consistency in the items in this study. Deleting any items would not increase reliability.

3.4.5. Critical thinking

Critical thinking is measured using the Computational Thinking Scale (CTS) by Korkmaz et al. (2017). The CTS consists out of 5 subscales; creativity, algorithmic thinking, cooperativity, problem-solving, and critical thinking. Critical thinking assesses individuals' ability to analyze information, make reasoned judgments, and approach problem-solving tasks with a critical mindset. It consists of 5 items, including "I am willing to learn challenging things." (Korkmaz et al, 2017, p. 565). The original

study measures the scale using a 5-point Likert scale, however, a 7-point Likert scale from 'strongly agree' to 'strongly disagree' was adopted in this study to keep the consistency in the survey. Research has shown no statistically significant differences in alpha and test-retest coefficients between the 5-point and 7-point Likert scales. Moreover, the reliability scores slightly increased as the number of response categories in the scale grew (Altuna & Arslan, 2016, p. 15).

The reliability analysis for critical thinking in this study showed that Cronbach's alpha was .79, indicating good internal consistency in the items in this study. Deleting any items would not increase reliability.

3.5. Analytical approach

After the survey was conducted, the analysis was done by analyzing the output with SPSS. SPSS is a statistically oriented computer program used for various purposes, including data collection, analysis, and visualization. SPSS is widely used in social sciences, education, and other fields for research and data analysis (Surfspot, n.d., p. 1). The cleaned dataset was tested on reliability doing reliability analysis for each subscale. The hypotheses were tested by doing various quantitative SPSS tests. To test H1 and H2, a linear regression analysis in SPSS was done. A linear regression analysis can be done to examine the relationship between an independent variable and a dependent variable (Bevans, 2023, p. 1).

To test the moderation effect hypotheses H3-H8 and the mediation effect hypothesis H9 and H10, PROCESS in SPSS was utilized. PROCESS, developed by Andrew F. Hayes, is a tool designed to handle both moderation and mediation analyses. This makes it ideal for testing complex models where both types of effects are hypothesized. PROCESS employs bootstrapping techniques to generate confidence intervals for indirect effects and conditional effects, enhancing the robustness and reliability of the findings. This reduces the likelihood of Type I and Type II errors, providing more accurate estimates. The macro allows for extensive customization, enabling researchers to specify complex models with multiple mediators and moderators (Hayes, 2023, p. 1).

The conclusion will be drawn from rejecting or accepting the proposed hypotheses in chapter 4 where the results of the study are discussed.

3.6. Reliability and validity

To enhance the reliability and validity of this research, previous research was analyzed and ensured the variables relied on established scales for each measurement as mentioned in the operationalization (3.4). These scales have been validated in original studies, which enhances the likelihood that the measurements in this study accurately reflect the intended concepts. By using these established scales, I aimed to ensure high construct validity.

For this research, existing scales for all measurements were used. These scales were reported to be reliable in the original studies, with documented Cronbach's alpha or composite reliability values.

To verify the reliability of these measurements in this research context, a reliability analysis for each variable used in the survey was conducted to ensure that the reliability was acceptable.

4. Results

The previous chapters, including the theoretical framework and the methodology section, form the foundation for this chapter, the results section. Here, the findings from various data analyses are presented that were conducted throughout the study.

4.1. Hypothesis testing: Regression analysis.

To test H1 and H2, where privacy concerns predict risk beliefs and attitude, two linear regression analyses were conducted for both hypotheses. First, a linear regression analysis was conducted with privacy concerns as the independent variable and with risk beliefs as the dependent variable (Table 4). The model was found to be significant, $F(1, 154) = 64.66$, $p < .001$, $R^2 = .30$. Privacy concerns were found to be a significant positive predictor of risk beliefs ($b^* = .55$, $t = 8.04$, $p < 0.001$, 95% *CI* [0.59, 0.98]), indicating that higher levels of privacy concerns are associated with higher levels of perceived risk. Specifically, for every one-unit increase in privacy concerns, the perceived risk increases by .78 units ($b = .78$). For all of these effects, it is assumed that the other independent variables remain constant. This result supports H1 indicating that privacy concerns are strongly positively associated with the risk beliefs of users towards LLMS and H1 is therefore accepted.

Additionally, a linear regression analysis was conducted with attitude as the dependent variable. The predictor was privacy concerns (Table 5). The model was not found to be significant, $F(1, 154) = 3.88$, $p = .051$, $R^2 = .03$. Privacy concerns were found to be a non-significant negative predictor of attitude ($b^* = -.16$, $t = -1.97$, $p = 0.051$, 95% *CI* [−0.39, −0.00]), providing no support for the hypothesis that privacy concerns are negatively associated with the attitude of users towards LLMs. Specifically, for every one-unit increase in privacy concerns, the attitude decreases by .20 units ($b = .20$). For all of these effects, it is assumed that the other independent variables remain constant. There is a weak negative correlation between privacy concerns and attitude, but this relationship is not statistically significant. This result does not support H2 indicating that privacy concerns are negatively associated with the attitude of users towards large language models and H2 is therefore rejected.

Table 4. Regression model for predicting risk beliefs.

Effect	Estimate	*SE*	95% CI		*p*
			LL	*UL*	
Model 1: Risk beliefs					
Intercept	1.19	.24	.72	1.65	<.001
Privacy concerns	.78	.10	.59	.98	<.001
Model summary					
R	.55				

R^2	.30				
Adjusted R^2	.29				
F	64.66				<.001

Note. Number of studies = 1, number of effects = 1, *N* = 155. CI = confidence interval; *LL* = lower limit; *UL* = upper limit.

Table 5. Regression model for predicting risk beliefs (*N* = 155)

Effect	Estimate	*SE*	95% CI		*p*
			LL	*UL*	
Model 2: Attitude					
Intercept	2.86	.24	2.39	3.34	<.001
Privacy concerns	-.20	.10	-.39	-.001	.051
Model summary					
R	.16				
R^2	.03				
Adjusted R^2	.02				
F	3.88				.051

Note. Number of studies = 1, number of effects = 1, *N* = 155. CI = confidence interval; *LL* = lower limit; *UL* = upper limit

4.2. Hypothesis testing: Moderation analysis

4.2.1. Moderation effects of AI literacy on the relationship between privacy concerns and risk beliefs

To test the moderation hypotheses H3-H5 moderation analyses were used using the PROCESS macro by Andrew F. Hayes (2023). First, a moderation analysis was conducted using the PROCESS macro with risk beliefs as the dependent variable, privacy concerns (PrivCon) as the independent variable, and technical understanding (LitTecUn) as the moderator (Table 6). The overall model was significant, $F(3, 151) = 23.72$, $p < .001$, $R^2 = .32$, suggesting that the predictors together significantly explain the variance in risk beliefs. Privacy concerns were a significant positive predictor of risk beliefs ($b = 1.09$, $SE = .28$, $t = 3.85$, $p < .001$, 95% CI [0.53, 1.65]), indicating that higher levels of privacy concerns are associated with higher levels of perceived risk. Technical understanding was not a significant predictor of risk beliefs ($b = .06$, $SE = .14$, $t = 0.41$, $p = .683$, 95% CI [-0.22, 0.34]). The interaction term between privacy concerns and technical understanding was not significant ($b = -.08$, $SE = .06$, $t = -1.22$, $p = .223$, 95% CI [-0.20, 0.05]), indicating that technical understanding does not significantly moderate the relationship between privacy concerns and risk beliefs. To probe the interaction effect, the simple slopes at ± 1 *SD* of the mean of technical understanding were examined

(Table 7). The results showed that at low levels of technical understanding (Mean - 1 *SD*), the effect of privacy concerns on risk beliefs was $b = 1.14$, $SE = .29$, $t = 3.93$, $p < .001$. At high levels of technical understanding (Mean + 1 *SD*), the effect of privacy concerns on risk beliefs was $b = 1.04$, $SE = .32$, $t = 3.25$, $p < .001$. These results show that higher privacy concerns are consistently associated with higher risk beliefs regardless of the level of technical understanding. Therefore, H3 is rejected.

Table 6. Moderation analysis of privacy concerns and risk beliefs by technical understanding ($N = 155$)

Predictor	*b*	*SE*	*t*	*p*	95% CI LL	95% CI UL
Constant	0.97	.68	1.44	.153	-0.36	2.31
Privacy concerns	1.09	.28	3.86	.0002	0.53	1.65
Technical understanding	0.06	.14	0.41	.683	-0.22	0.34
Privacy concerns x Tech. Und.	-.08	.06	-1.22	.223	-0.20	0.05

Table 7. Conditional effects of technical understanding on risk beliefs

Technical understanding	Effect	*SE*	*t*	*p*	95% CI Low	95% CI Up
-1 SD	1.14	.29	3.93	<.001	0.57	1.71
Mean	1.09	.28	3.86	.0002	0.53	1.65
+1 SD	1.04	.32	3.25	<.001	0.41	1.67

Second, a moderation analysis was conducted using the PROCESS macro with risk beliefs as the dependent variable, privacy concerns (PrivCon) as the independent variable, and critical appraisal (LitCriAp) as the moderator. The overall model was significant, $F(3, 151) = 21.84$, $p < .001$, $R^2 = .30$, suggesting that the predictors together significantly explain the variance in risk beliefs (Table 8). Privacy concerns were a significant positive predictor of risk beliefs ($b = .88$, $SE = .26$, $t = 3.39$, $p < .001$, 95% CI [0.37, 1.40]), indicating that higher levels of privacy concerns are associated with higher levels of risk beliefs. Critical appraisal was not a significant predictor of risk beliefs ($b = -.02$, $SE = 0.19$, $t = -0.10$, $p = .919$, 95% CI [-0.39, 0.35]). The interaction term between privacy concerns and critical appraisal was not significant ($b = -.03$, $SE = 0.08$, $t = -0.35$, $p = .725$, 95% CI [-0.20, 0.14]), indicating that critical appraisal does not significantly moderate the relationship between privacy concerns and risk beliefs. To probe the interaction effect, the simple slopes at ± 1 *SD* of the mean of critical appraisal were examined (Table 9). The results showed that at low levels of critical appraisal (Mean - 1 *SD*), the effect of privacy concerns on risk beliefs was $b = .91$, $SE = .27$, $t = 3.37$, $p < .001$.

At high levels of critical appraisal (Mean + 1 *SD*), the effect of privacy concerns on risk beliefs was $b = .85$, $SE = .28$, $t = 3.03$, $p < .001$. These results show that higher privacy concerns are consistently associated with higher risk beliefs regardless of the level of critical appraisal. Therefore, H4 is rejected.

Table 8. Moderation analysis of privacy concerns and risk beliefs by critical appraisal ($N = 155$)

Predictor	*b*	*SE*	*t*	*p*	95% CI LL	95% CI UL
Constant	1.20	.57	2.12	.036	0.08	2.32
Privacy concerns	0.88	.26	3.39	.0009	0.37	1.40
Critical appraisal	-0.02	.19	-0.10	.919	-0.39	0.35
Privacy concerns x Crit. App.	-0.03	.08	-0.35	.725	-0.20	0.14

Table 9. Conditional effects of critical appraisal on risk beliefs

Critical appraisal	Effect	*SE*	*t*	*p*	95% CI Low	95% CI Up
-1 SD	0.91	.27	3.37	<.001	0.37	1.45
Mean	0.88	.26	3.39	.0009	0.37	1.40
+1 SD	0.85	.28	3.03	<.001	0.29	1.41

Lastly, for the moderation effects on risk beliefs, a moderation analysis was conducted using the PROCESS macro with risk beliefs as the dependent variable, privacy concerns (PrivCon) as the independent variable, and practical application (LitPraAp) as the moderator. The overall model was significant, $F(3, 151) = 21.76$, $p < .001$, $R^2 = .30$, suggesting that the predictors together significantly explain the variance in risk beliefs (Table 10). Privacy concerns were a significant positive predictor of risk beliefs ($b = .60$, $SE = .26$, $t = 2.32$, $p = .022$, 95% CI [0.09, 1.11]), indicating that higher levels of privacy concerns are associated with higher levels of perceived risk. Practical application was not a significant predictor of risk beliefs ($b = -.20$, $SE = .21$, $t = -0.96$, $p = .338$, 95% CI [-0.62, 0.21]). The interaction term between privacy concerns and practical application was not significant ($b = .07$, $SE = .09$, $t = 0.77$, $p = .443$, 95% CI [-0.11, 0.25]), indicating that practical application does not significantly moderate the relationship between privacy concerns and risk beliefs. To probe the interaction effect, the simple slopes at ± 1 *SD* of the mean of practical application were examined (Table 11). The results showed that at low levels of practical application (Mean - 1 *SD*), the effect of privacy concerns on risk beliefs was $b = .67$, $SE = .28$, $t = 2.39$, $p = .018$. At high levels of practical application (Mean + 1 *SD*), the effect of privacy concerns on risk beliefs was $b = .53$, $SE = .29$, $t = 1.83$, $p = .069$. These results suggest that higher privacy concerns are consistently associated with

higher risk beliefs regardless of the level of practical application. Therefore, H5 is rejected and no significant moderation effect was found for the relationship between privacy concerns and risk beliefs.

Table 10. Moderation analysis of privacy concerns and risk beliefs by practical application (*N* = 155)

Predictor	*b*	*SE*	*t*	*p*	95% CI LL	95% CI UL
Constant	1.72	.61	2.84	.005	0.52	2.92
Privacy concerns	0.60	.26	2.32	.022	0.09	1.11
Practical application	-0.20	.21	-0.96	.338	-0.62	0.21
Privacy concerns x Pract. App.	0.07	.09	0.77	.443	-0.11	0.25

Table 11. Conditional effects of practical application on risk beliefs

Practical application	Effect	*SE*	*t*	*p*	95% CI Low	95% CI Up
-1 SD	0.67	.28	2.39	.018	0.12	1.22
Mean	0.60	.27	2.24	.027	0.07	1.14
+1 SD	0.53	.29	1.83	.069	-0.04	1.10

4.2.2. Moderation effects of AI literacy on the relationship between privacy concerns and attitude

To test the moderation hypotheses H6-H8 moderation analyses were used using the PROCESS macro by Andrew F. Hayes (2023). First, a moderation analysis was conducted using the PROCESS macro with attitude as the dependent variable, privacy concerns (PrivCon) as the independent variable, and technical understanding (LitTecUn) as the moderator. The overall model was not significant, $F(3, 151) = 2.16$, $p = .095$, $R^2 = .04$, suggesting that the predictors together do not significantly explain the variance in attitude (Table 12). Privacy concerns were not a significant predictor of attitude ($b = .01$, $SE = .29$, $t = 0.02$, $p = .981$, 95% CI [-0.57, 0.58]). Technical understanding was not a significant predictor of attitude ($b = .18$, $SE = 0.15$, $t = 1.19$, $p = .236$, 95% CI [-0.12, 0.47]). The interaction term between privacy concerns and technical understanding was not significant ($b = -.04$, $SE = .06$, $t = -0.69$, $p = .490$, 95% CI [-0.17, 0.08]), indicating that technical understanding does not significantly moderate the relationship between privacy concerns and attitude. To probe the interaction effect, the simple slopes at ± 1 *SD* of the mean of technical understanding were examined (Table 13). The results showed that at low levels of technical understanding (Mean - 1 *SD*), the effect of privacy concerns on attitude was $b = -.04$, $SE = .34$, $t = -0.12$, $p = .907$. At high levels of technical understanding (Mean + 1 *SD*), the effect of privacy concerns on attitude was $b = 0.05$, $SE = .34$, $t = 0.15$, $p = .881$. These

results show that neither privacy concerns nor technical understanding have a significant impact on attitude, and there is no significant moderation effect of technical understanding on the relationship between privacy concerns and attitude. Therefore, H6 is rejected.

Table 12. Moderation analysis of privacy concerns and attitude by technical understanding (N = 155)

Predictor	*b*	*SE*	*t*	*p*	95% CI LL	95% CI UL
Constant	2.06	.70	2.97	.003	0.69	3.44
Privacy concerns	0.01	.29	0.02	.981	-0.57	0.58
Technical understanding	0.18	.15	1.19	.236	-0.12	0.47
Privacy concerns x Tech. Und.	-0.04	.06	-0.69	.490	-0.17	0.08

Table 13. Conditional effects of technical understanding on attitude

Technical understanding	Effect	*SE*	*t*	*p*	95% CI Low	95% CI Up
-1 SD	-0.04	.34	-0.12	.907	-0.71	0.63
Mean	0.01	.29	0.04	.981	-0.57	0.58
+1 SD	0.05	.34	0.15	.881	-0.63	0.73

Second, a moderation analysis was conducted using the PROCESS macro with attitude as the dependent variable, privacy concerns (PrivCon) as the independent variable, and critical appraisal (LitCriAp) as the moderator. Interestingly, the overall model was significant, $F(3, 151) = 6.26$, $p < .001$, $R^2 = .11$, suggesting that the predictors together significantly explain the variance in attitude (Table 14). Privacy concerns were a significant negative predictor of attitude (b = -.81, SE = 0.25, t = -3.18, p = .002, 95% CI [-1.31, -0.31]), indicating that higher privacy concerns are associated with lower attitude scores. Critical appraisal was not a significant predictor of attitude (b = -.19, SE = 0.18, t = -1.01, p = .313, 95% CI [-0.55, 0.18]). The interaction term between privacy concerns and critical appraisal was significant (b = .20, SE = 0.08, t = 2.43, p = .016, 95% CI [0.04, 0.36]), indicating that critical appraisal significantly moderates the relationship between privacy concerns and attitude. Conditional effects analysis revealed that the negative effect of privacy concerns on attitude is significant at low and mean levels of critical appraisal, but becomes non-significant at high levels of critical appraisal (Table 15). This suggests that higher levels of critical appraisal can mitigate the negative impact of privacy concerns on attitude. Specifically, at low levels of critical appraisal (Mean - 1 *SD*), the effect of privacy concerns on attitude was b = -.47, SE = .14, t = -3.45, $p < .001$, 95% CI [-0.73, -0.20]. At mean levels of critical appraisal, the effect was b = -.26, SE = .10, t = -2.65, p = .009,

95% CI [-0.45, -0.06]. At high levels of critical appraisal (Mean + 1 *SD*), the effect was not significant (*b* = -.05, *SE* = .12, *t* = -0.37, *p* = .712, 95% CI [-0.29, 0.20]). These results show that while higher privacy concerns are associated with lower attitude scores, critical appraisal can reduce this negative impact. Therefore, H7 is accepted.

Table 14. Moderation analysis of privacy concerns and attitude by critical appraisal (*N* = 155)

Predictor	*b*	*SE*	*t*	*p*	95% CI LL	95% CI UL
Constant	3.49	.56	6.28	.000	2.40	4.59
Privacy concerns	-0.81	.25	-3.18	.002	-1.31	-0.31
Critical appraisal	-0.19	.18	-1.01	.313	-0.55	0.18
Privacy Concerns x Crit. App.	0.20	.08	2.43	.016	0.04	0.36

Table 15. Conditional effects of critical appraisal on attitude

Critical appraisal	Effect	*SE*	*t*	*p*	95% CI Low	95% CI Up
-1 SD	-0.47	.14	-3.45	<.001	-0.73	-0.20
Mean	-0.26	.10	-2.65	.009	-0.45	-0.06
+1 SD	-0.05	.12	-0.37	.712	-0.29	0.20

Lastly, a moderation analysis was conducted using the PROCESS macro with attitude as the dependent variable, privacy concerns as the independent variable, and practical application (LitPraAp) as the moderator. The overall model was significant, $F(3, 151) = 13.38$, $p < .001$, $R^2 = .21$, suggesting that the predictors together significantly explain the variance in attitude (Table 16). Privacy concerns were a significant negative predictor of attitude (*b* = -.64, *SE* = .24, *t* = -2.71, *p* = .008, 95% CI [-1.11, -0.17]), indicating that higher privacy concerns are associated with lower attitude scores. Practical application was not a significant predictor of attitude (*b* = .03, *SE* = .20, *t* = 0.15, *p* = .881, 95% CI [-0.36, 0.42]). The interaction term between privacy concerns and practical application was significant (*b* = .18, *SE* = .08, *t* = 2.13, *p* = .035, 95% CI [0.01, 0.34]), indicating that practical application significantly moderates the relationship between privacy concerns and attitude. Conditional effects analysis revealed that the negative effect of privacy concerns on attitude is significant at low levels of practical application, marginally significant at the mean level, and becomes non-significant at high levels of practical application (Table 17). This suggests that higher levels of practical application can mitigate the negative impact of privacy concerns on attitude. Specifically, at low levels of practical application (Mean - 1 *SD*), the effect of privacy concerns on attitude was *b* = -.35, *SE* = .12, *t* = -2.88, *p* = .004, 95% CI [-0.59, -0.11]. At mean levels of practical application, the effect was *b* = -.18, *SE* =

.09, t = -1.95, p = .054, 95% CI [-0.35, 0.00]. At high levels of practical application (Mean + 1 *SD*), the effect was not significant (b = .00, SE = .12, t = 0.02, p = .988, 95% CI [-0.24, 0.25]). These results show that while higher privacy concerns are associated with lower attitude scores, practical application can reduce this negative impact. Therefore, H8 is accepted.

Table 16. Moderation analysis of privacy concerns and attitude by practical application (N = 155)

Predictor	*b*	*SE*	*t*	*p*	95% CI LL	95% CI UL
Constant	2.75	.56	4.90	.000	1.64	3.85
Privacy concerns	-0.64	.24	-2.71	.008	-1.11	-0.17
Practical application	0.03	.20	0.15	.881	-0.36	0.42
Privacy concerns x Pract. App.	0.18	.08	2.13	.035	0.01	0.34

Table 17. Conditional effects of practical application on attitude

Practical application	Effect	*SE*	*t*	*p*	95% CI Low	95% CI Up
-1 SD	-0.35	.12	-2.88	.004	-0.59	-0.11
Mean	-0.18	.09	-1.95	.054	-0.35	0.00
+1 SD	0.00	.12	0.02	.988	-0.24	0.25

4.3. Hypothesis testing: Mediation analysis

To test hypotheses H9 and H10, a mediation analysis using PROCESS macro by Andrew F. Hayes (2023) was employed. First, a bootstrapping procedure was employed to test for a possible mediation effect (Preacher & Hayes, 2004), in which privacy concerns was entered as the independent variable, critical thinking as the mediator, and risk beliefs as the dependent variable (Table 18 & 19). The analysis was conducted with 155 participants. Privacy concerns had a significant effect on critical thinking (b = .25, SE = .08, t = 3.13, p = .002, 95% CI [0.09, 0.41]), indicating that higher privacy concern was associated with higher levels of critical thinking. Critical thinking did not significantly influence risk beliefs (b = .12, SE = .10, t = 1.24, p = .218, 95% CI [-0.07, 0.31]), whereas privacy concern significantly influenced risk beliefs (b = .75, SE = .10, t = 7.50, p < .001, 95% CI [0.55, 0.95]). The indirect effect of privacy concern on risk beliefs through critical thinking was not significant (β = 0.03, *BootSE* = .04, 95% CI = [-0.02, 0.12]. This shows that H9 suggesting the mediation effect of critical thinking on the relationship between privacy concern and risk was not supported and H9 is rejected.

Table 18. Results of mediation analysis for risk beliefs and attitude

Antecedent	M (Critical thinking)	Y (Risk beliefs)	Y (Attitude)
	b		*SE*
X (Privacy concerns)	0.25		.08
M (Critical thinking)	-		-
R^2	0.06		-
F (df1, df2)	9.82		-

Table 19. Indirect effect of privacy concerns on risk beliefs through critical thinking

IV	M	DV	Effect	*BootSE*	*BootLLCI*	*BootULCI*	*p*
Privacy concerns	Critical thinking	Risk beliefs	0.03	0.04	-0.02	0.12	.218

Note: IV = independent variable, M = mediator, DV = dependent variable

Second, a bootstrapping procedure was employed to test for a possible mediation effect (Preacher & Hayes, 2004), in which privacy concerns was entered as the independent variable, critical thinking as the mediator, and attitude as the dependent variable. The analysis was conducted with 155 participants. Privacy concern had a significant effect on critical thinking (b = .25, SE = .08, t = 3.13, p = .002, 95% CI [0.09, 0.41]), indicating that higher privacy concern was associated with higher levels of critical thinking (Table 18). Critical thinking significantly influenced attitude (b = .45, SE = .09, t = 4.83, p < .001, 95% CI [0.26, 0.63]), while privacy concern had a significant negative effect on attitude (b = −.31, SE = 0.10, t = -3.23, p = .002, 95% CI [-0.50, -0.12]). The indirect effect of privacy concern on attitude through critical thinking was significant (β = 0.11, *BootSE* = .06, 95% *CI*= [0.02, 0.23]) (Table 20). This suggests that critical thinking partially mediates the relationship between privacy concern and attitude. In other words, while part of the effect of privacy concern on attitude is explained by the mediator, there is still a direct effect of privacy concern on attitude that is not accounted for by the mediator. Thus, H10 is accepted.

Table 20. Indirect effects of privacy concerns on attitude through critical thinking

IV	M	DV	Effect	*BootSE*	*BootLLCI*	*BootULCI*	*p*
Privacy concerns	Critical thinking	Attitude	0.11	0.06	0.02	0.23	0.002

Note: IV = independent variable, M = mediator, DV = dependent variable

The following table shows an overview of the accepted and rejected hypotheses.

Table 21. Results overview

	Hypothesis	Results
H1	Privacy concerns are positively associated with the risk beliefs of users towards large language models.	Accepted
H2	Privacy concerns are negatively associated with users' attitude toward large language models.	Rejected
H3	The positive relationship between privacy concerns and the risk beliefs of people using large language models is weaker for users who score higher on technical understanding of AI.	Rejected
H4	The positive relationship between privacy concerns and the risk beliefs of people using large language models is weaker for users who score higher on critical appraisal of AI.	Rejected
H5	The positive relationship between privacy concerns and the risk beliefs of people using large language models is weaker for users who score higher on practical application AI.	Rejected
H6	The negative relationship between privacy concerns and the attitude of people using large language models is weaker for users who score higher on technical understanding of AI.	Rejected
H7	The negative relationship between privacy concerns and the attitude of people using large language models is weaker for users who score higher higher critical appraisal of AI.	Accepted
H8	The negative relationship between privacy concerns and the attitude of people using large language models is weaker for users who score higher on practical application of AI.	Accepted
H9	Critical thinking will mediate the positive relationship between privacy concerns and the risk beliefs of people using large language models.	Rejected
H10	Critical thinking will mediate the negative relationship between privacy concerns and the attitude of people using large language models.	Accepted

5. Conclusion and discussion

This final chapter synthesizes the findings from the previous chapters, addressing the central research question and discussing the theoretical and practical implications of the study. The limitations of the study are discussed as well as recommendations for future research.

5.1. Main findings

The central question of this research was: "To what extent do AI literacy moderate and critical thinking mediate the relationship between privacy concerns and the perceived risk and attitude of large language model users?". The findings from this research show that privacy concerns influence both risk beliefs and attitudes toward LLMs. Privacy concerns significantly and positively impact risk beliefs, suggesting that individuals with higher privacy concerns perceive greater risks when using LLMs. However, privacy concerns have a weak negative correlation with attitudes toward LLMs, though this relationship was not statistically significant. Critical thinking was found to partially mediate the relationship between privacy concerns and attitude but did not mediate the relationship between privacy concerns and risk beliefs. Additionally, AI literacy and its subscales were tested as moderators, but only critical appraisal and practical application dimensions significantly moderated the relationship between privacy concerns and attitudes, managing the negative impact of privacy concerns on attitudes toward LLMs. Technical understanding did not significantly moderate the relationship between privacy concerns and attitude.

5.2. Theoretical implications

The research enriches the understanding of the IUIPC model by Malhotra et al. (2004) within the context of LLMs. The positive relationship between privacy concerns and risk beliefs supports the IUIPC model, which suggests that higher privacy concerns lead to heightened risk beliefs. This is consistent with previous studies (Gurung & Raja, 2016; Kim et al., 2023; Koohang et al., 2018). This implies that users of LLMs are more likely to perceive higher risks while utilizing these models if they have more privacy concerns. They could be concerned, for instance, that the AI systems would abuse, disclose, or manage their personal data improperly. These consumers are cautious of giving LLMs access to their personal information because they fear that there could be privacy-related problems. As a result, their elevated risk beliefs may affect how they behave and think about LLMs, which may result in decreased usage rates, a rise in the need for privacy measures, or a greater call for technologies that protect privacy. This knowledge shows how crucial it is for developers and legislators to successfully handle privacy concerns in order to build trust and promote the adoption of LLMs.

The relationship between privacy concerns and attitudes towards LLMs, although negative, was not statistically significant, challenging some of the previous findings that indicated a strong negative correlation between privacy concerns and attitudes toward AI technologies (Ketelaar & Van

Balen, 2018; Pitardi & Marriott, 2021). This suggests that other factors might be influencing attitudes toward LLMs, and these should be explored further. The privacy paradox might be one reason for this disparity. As previously mentioned, the privacy paradox occurs when people express strong worries about their privacy yet do not always act on those concerns (Norberg et al., 2007, p. 101). People frequently engage in activities that jeopardize their personal information, such as using online services and exchanging personal data freely, even when they claim to be concerned about their privacy (Norberg et al., 2007, p. 106-107). Users may be aware of and voice concerns regarding privacy threats in the context of LLMs, but these worries may not substantially change their views toward LLMs in general since they still find the technology to be very useful and handy. For example, their concerns about privacy may be outweighed by the benefits that LLMs offer in terms of efficiency, information access, and job automation, resulting in ongoing usage and positive attitudes. Therefore, the lack of statistical significance in the association between privacy concerns and attitudes toward LLMs could be attributed to the privacy paradox. Future studies should examine the privacy paradox's complexity in greater detail in the context of LLMs, as well as other elements that may affect users' attitudes toward LLMs, such as the advantages users perceive, their level of confidence in technology providers, and the privacy policies of LLM developers.

The introduction of AI literacy and critical thinking into the IUIPC model framework provides new insights. Critical thinking partially mediated the relationship between privacy concerns and attitude, highlighting its importance in how users process and respond to privacy concerns. This aligns with Kokolakis' (2017) call for more empirical research on cognitive abilities in the context of privacy concerns. This suggests that, in the face of privacy issues, users' attitudes toward LLMs are influenced by their critical thinking skills. More specifically, users with greater critical thinking abilities are better able to assess, consider, and understand the consequences of privacy concerns related to LLMs. Their capacity to think more clearly and critically about technology allows them to soften the negative impact of privacy worries on their attitudes. For example, a user with strong critical thinking skills could be aware of the possible privacy concerns associated with using an LLM, but they might also balance those risks against the advantages of using LLMs, such as increased productivity and information access. This balanced evaluation may result in a more nuanced perspective that is not primarily motivated by privacy issues. Consequently, while privacy concerns may typically result in more unfavorable attitudes regarding LLMs, the influence of these worries might be reduced by the availability of good critical thinking abilities, leading to less negative or even neutral attitudes.

The moderating effects of AI literacy, specifically critical appraisal and practical application, on the relationship between privacy concerns and attitude, suggest that higher AI literacy can soften the negative impact of privacy concerns on attitudes toward LLMs. This finding aligns with previous research suggesting that AI literacy influences users' understanding and perceptions of AI technologies (Ng et al., 2021, p. 2). It offers insight into the importance of ensuring users have the skills and knowledge needed to critically evaluate LLM and apply them effectively in practical contexts. Users

with higher AI literacy are better able to understand and manage potential privacy risks, leading to more positive or less negative attitudes towards LLMs. This means that individuals who have a higher degree of AI literacy, specifically critical appraisal and practical application, are better able to understand the nuances of AI technology, including possible advantages and disadvantages.

However, technical understanding, a subscale of the AI literacy scale did not emerge as a significant moderator in this study. This means that understanding the technical aspects of how AI and LLMs work does not significantly influence how privacy concerns affect users' attitudes toward these technologies. In other words, having technical knowledge alone does not help users feel more positive or less negative about LLMs when they have privacy concerns. There are some possible explanations for this. First, technical understanding might not directly influence how individuals perceive LLMs. While a technical understanding of AI could help users understand how these systems work in a more comprehensive way, it does not necessarily translate to a greater ability to assess privacy risks or form attitudes toward the use of these technologies. Privacy concerns and attitudes are often more influenced by experiences and the perceived risks of sharing the data rather than by in-depth technical knowledge (Pitardi & Marriott, 2021, p. 635). Additionally, another possible explanation could be that the subscale of technical understanding might be overly specific, as it asks for very specialized knowledge of AI. Users may not have the extensive technical understanding that this subscale measures, even when they might have a relatively high level of AI literacy. Consequently, the impact of technical understanding on privacy concerns and attitudes could be less significant compared to more relatable aspects of AI literacy, like critical appraisal and practical application, which are directly relevant to everyday use and understanding of LLMs and therefore significant moderators in this study. Future research could specifically focus on comparing people with high technical understanding of AI and individuals with lower technical understanding of AI or try different scales that measure AI literacy to further explore this.

Critical appraisal skills enable users to critically assess the reliability, credibility, and biases of AI technology and the information it generates. Users can evaluate the outputs of LLMs with a more informed perspective, recognizing when the information might be biased or unreliable. This critical evaluation helps users to trust the technology appropriately, balancing the benefits against the potential risks (Laupichler et al., 2023, p. 6). Therefore, it can be concluded that users with strong critical appraisal skills are less likely to be affected by their privacy concerns toward their attitude, as they can accurately evaluate and manage these concerns. Practical application skills involve the ability to use AI tools effectively and use them to solve real-world problems while at the same time implementing privacy-preserving techniques (Laupichler et al., 2023, p. 6). Users with high practical application skills can navigate the privacy settings of LLMs, understand the implications of data input, and apply best practices to protect their personal information. Therefore, it can be concluded that users with strong practical application skills are less likely to be affected by their privacy concerns toward their attitude, as they can navigate the privacy settings of LLMs, understand the implications of data

input, and apply best practices to protect their personal information. In the context of the existing literature on privacy concerns and attitude towards AI, it can be concluded that critical appraisal and practical application skills are moderators in this relationship. This can be explained by the IUIPC model by Malhotra et al. (2004), as critical appraisal and practical application skills are likely to enhance 'awareness of privacy practices' and 'perceived control', both subscales of measuring privacy concerns. Awareness of privacy practices' describes worries about communication and transparency around the use of personal data, which is similar to critical appraisal. Control refers to worries about being able to manage and alter personal information kept in databases, which is similar to practical application (Malhotra et al., 2004, p. 352).

5.3. Practical implications

The findings have several practical implications for organizations and developers of LLMs. First, organizations should prioritize addressing privacy concerns by enhancing transparency and control over personal data. Clear communication about data practices can help manage users' privacy concerns and reduce risk beliefs. Second, developing and implementing AI literacy programs can empower users to better understand and navigate AI technologies. Educating users about the capabilities and limitations of AI can help installing more positive attitudes and reduce unnecessary privacy concerns. Lastly, enhancing users' critical thinking skills could be a valuable strategy in addressing privacy concerns and fostering more positive attitudes towards LLMs and similar technologies. Educational programs or other interventions that help in developing critical thinking skills could therefore play a significant role in helping users navigate privacy issues more effectively.

5.4. Limitations and future research

Despite the valuable insights provided by this research, there are some limitations. The study relied on a convenience sample of 155 participants, which may not represent the broader population of LLM users. Future research should aim for a larger, more diverse sample to enhance generalizability and even conduct studies with more diverse populations, including different age groups, cultural backgrounds, and levels of AI exposure, to enhance the generalizability of the findings. Additionally, due to time and resource constraints, the literature review did not examine studies written in languages other than English. By examining studies written in other languages the relationship between privacy concerns, risk beliefs, attitudes, AI literacy and critical thinking can be analyzed in a more thorough perspective. Longitudinal studies are needed to explore how privacy concerns, risk beliefs, and attitudes evolve over time. Furthermore, the reliance on self-reported data may introduce biases such as social desirability bias or might not reflect reality. Future studies could incorporate objective measures or behavioral data to validate the findings. For example, measuring participants' critical thinking skills or other cognitive abilities assessed through standardized tests or behavioral tasks. This could provide a more accurate and robust understanding of their impact on privacy concerns, risk

beliefs, and attitudes towards LLMs. Future research could investigate other potential mediators and moderators, such as user experience and trust in technology to gain a more comprehensive understanding of the factors influencing attitudes toward LLMs. Lastly, this study included measuring risk beliefs. It is crucial to acknowledge that the manner in which a risk is constituted may influence the conclusions drawn. Therefore, future research should study the differential valuation of risks based on their probabilistic and impact components. Understanding these nuances can provide deeper insights into managing risk beliefs for LLMs.

References

Ahmed, S., & Lee, S. (2023). The inhibition effect: Privacy concerns disrupt the positive effects of social media use on online political participation. *New Media & Society*, 146144482311733. https://doi.org/10.1177/14614448231173328

Altuna, O. K., & Arslan, F. (2016). Impact of the number of scale points on data characteristics and respondents' evaluations: An experimental design approach using 5-Point and 7-Point Likert-type scales. *İstanbul Üniversitesi Siyasal Bilgiler Fakültesi Dergisi/İstanbul Üniversitesi Siyasal Bilgiler Fakültesi Dergisi*, *55*, 1–20. https://doi.org/10.17124/iusiyasal.320009

Ambrosio, A. P., Macedo, J., Almeida, L. D. S., & Franco, A. (2014). *Exploring core cognitive skills of computational thinking*. http://users.sussex.ac.uk/~bend/ppig2014/3ppig2014_submission_13.pdf

Ashoori, M., & Weisz, J. D. (2019). In AI we trust? Factors that influence trustworthiness of AI-infused Decision-Making processes. *arXiv (Cornell University)*. https://arxiv.org/pdf/1912.02675.pdf

Babbie, E. R. (2016). *The basics of social research* (7th ed.). Wadsworth Publishing Co Inc. https://ci.nii.ac.jp/ncid/BB12429869

Baidoo-Anu, D., & Ansah, L. O. (2023). Education in the Era of Generative Artificial Intelligence (AI): Understanding the potential benefits of ChatGPT in promoting teaching and learning. *Journal of AI*, *7*(1), 52–62. https://doi.org/10.2139/ssrn.4337484

Bernabei, M., Colabianchi, S., Falegnami, A., & Costantino, F. (2023). Students' use of large language models in engineering education: A case study on technology acceptance, perceptions, efficacy, and detection chances. *Computers and Education: Artificial Intelligence*, *5*, 100172. https://doi.org/10.1016/j.caeai.2023.100172

Bevans, R. (2023, June 22). *Multiple Linear Regression | A Quick Guide (Examples)*. Scribbr. https://www.scribbr.com/statistics/multiple-linear-regression/

Bitkina, O. V., Jeong, H., Lee, B. C., Park, J., Park, J., & Kim, H. K. (2020). Perceived trust in artificial intelligence technologies: A preliminary study. *Human Factors and Ergonomics in Manufacturing & Service Industries*, *30*(4), 282–290. https://doi.org/10.1002/hfm.20839

Brough, A. R., & Martin, K. D. (2020). Critical roles of knowledge and motivation in privacy research. *Current Opinion in Psychology*, *31*, 11–15. https://doi.org/10.1016/j.copsyc.2019.06.021

Çelik, İ. (2023). Exploring the determinants of artificial intelligence (AI) literacy: digital divide, computational thinking, cognitive absorption. *Telematics and Informatics*, *83*, 102026. https://doi.org/10.1016/j.tele.2023.102026

Chai, C. S., Wang, X., & Xu, C. (2020). An extended theory of planned behavior for the modelling of Chinese secondary school students' intention to learn artificial intelligence. *Mathematics*, *8*(11), 2089. https://doi.org/10.3390/math8112089

Dawes, J. (2008). Do data characteristics change according to the number of scale points used? An experiment using 5-Point, 7-Point and 10-Point scales. *International Journal of Market Research*, *50*(1), 61–104. https://doi.org/10.1177/147078530805000106

Dinev, T., Hart, P., & Mullen, M. R. (2008). Internet privacy concerns and beliefs about government surveillance – An empirical investigation. *The Journal of Strategic Information Systems*, *17*(3), 214–233. https://doi.org/10.1016/j.jsis.2007.09.002

Eagly, A., & Chaiken, S. (1998). *The Handbook of Social Psychology: Attitude structure and function* (D. T. Gilbert, S. T. Fiske, & G. Lindzey, Eds.; Vol. 1). Oxford University Press.

Fortes, N., Rita, P., & Pagani, M. (2017). The effects of privacy concerns, perceived risk and trust on online purchasing behaviour. *International Journal of Internet Marketing and Advertising*, *11*(4), 307. https://doi.org/10.1504/ijima.2017.087269

Grassini, S. (2023). Development and validation of the AI attitude scale (AIAS-4): a brief measure of general attitude toward artificial intelligence. *Frontiers in Psychology*, *14*. https://doi.org/10.3389/fpsyg.2023.1191628

Gurung, A., & Raja, M. K. (2016). Online privacy and security concerns of consumers. *Information & Computer Security/Information and Computer Security*, *24*(4), 348–371. https://doi.org/10.1108/ics-05-2015-0020

Halpern, D. F. (1989). *Thought and Knowledge: An Introduction to Critical thinking*. https://ci.nii.ac.jp/ncid/BA6257521X

Halpern, D. F. (2014). *Thought and knowledge: An Introduction to Critical Thinking* (5th ed.). Psychology Press.

ISBN: 978-1-84872-628-4

Hasan, R., Shams, S. M. R., & Rahman, M. (2021). Consumer trust and perceived risk for voice-controlled artificial intelligence: The case of Siri. *Journal of Business Research*, *131*, 591–597. https://doi.org/10.1016/j.jbusres.2020.12.012

Hayes, A. F. (2023). *PROCESS macro for SPSS, SAS, and R*. processmacro.org. https://www.processmacro.org/index.html

Holmes, W., Council of Europe, Persson, J., Chounta, I. A., Wasson, B., & Dimitrova, V. (2022). *Artificial intelligence and education: A Critical View Through the Lens of Human Rights, Democracy and the Rule of Law*. Council of Europe Publishing.

ISTE & CSTA. (2011). *Computational Thinking in K–12 Education Leadership Toolkit.* ISTE. https://cdn.iste.org/www-root/2020-10/ISTE_CT_Leadership_Toolkit_booklet.pdf?_ga=2.52886048.907063893.1714828848-2006523725.1714828847

James, T., & Bélanger, F. (2020). A Theory of Multilevel Information Privacy Management for the Digital Era. *Information Systems Research*, *31*(2), 510–536. https://doi.org/10.1287/isre.2019.0900

Jo, H., & Park, D. (2024). Effects of ChatGPT's AI capabilities and human-like traits on spreading information in work environments. *Scientific Reports*, *14*(1). https://doi.org/10.1038/s41598-024-57977-0

Kelly, S., Kaye, S., & Oviedo-Trespalacios, Ó. (2023). What factors contribute to the acceptance of artificial intelligence? A systematic review. *Telematics and Informatics*, *77*, 101925. https://doi.org/10.1016/j.tele.2022.101925

Ketelaar, P., & Van Balen, M. (2018). The smartphone as your follower: The role of smartphone literacy in the relation between privacy concerns, attitude and behaviour towards phone-embedded tracking. *Computers in Human Behavior*, *78*, 174–182. https://doi.org/10.1016/j.chb.2017.09.034

Kim, Y., Kim, S. H., Peterson, R. A., & Choi, J. (2023). Privacy concern and its consequences: A meta-analysis. *Technological Forecasting & Social Change/Technological Forecasting and Social Change*, *196*, 122789. https://doi.org/10.1016/j.techfore.2023.122789

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, *64*, 122–134. https://doi.org/10.1016/j.cose.2015.07.002

Koohang, A., Paliszkiewicz, J., & Gołuchowski, J. (2018). Social media privacy concerns: trusting beliefs and risk beliefs. *Industrial Management + Data Systems/Industrial Management & Data Systems*, *118*(6), 1209–1228. https://doi.org/10.1108/imds-12-2017-0558

Korkmaz, Ö., Akir, R., & Zden, M. Y. (2017). A validity and reliability study of the computational thinking scales (CTS). *Computers in Human Behavior*, *72*, 558–569. https://doi.org/10.1016/j.chb.2017.01.005

Laupichler, M. C., Aster, A., Haverkamp, N., & Raupach, T. (2023). Development of the "Scale for the assessment of non-experts' AI literacy" – An exploratory factor analysis. *Computers in Human Behavior Reports*, *12*, 100338. https://doi.org/10.1016/j.chbr.2023.100338

Lee, I., Ali, S., Zhang, H., DiPaola, D., & Breazeal, C. (2021). Developing Middle School Students' AI Literacy. *SIGCSE '21: Proceedings of the 52nd ACM Technical Symposium on Computer Science Education*. https://doi.org/10.1145/3408877.3432513

Lund, B., & Wang, T. (2023). Chatting about ChatGPT: how may AI and GPT impact academia and libraries? *Library Hi Tech News*, *40*(3), 26–29. https://doi.org/10.1108/lhtn-01-2023-0009

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet Users' Information Privacy Concerns (IUIPC): the construct, the scale, and a causal model. *Information Systems Research*, *15*(4), 336–355. https://doi.org/10.1287/isre.1040.0032

Marr, B. (2023, May 19). A short history of ChatGPT: How we got to where we are today. *Forbes*. https://www.forbes.com/sites/bernardmarr/2023/05/19/a-short-history-of-chatgpt-how-we-got-to-where-we-are-today/

Murphy, K., Di Ruggiero, E., Upshur, R., Willison, D. J., Malhotra, N., Cai, J., Malhotra, N., Lui, V., & Gibson, J. L. (2021). Artificial intelligence for good health: a scoping review of the ethics literature. *BMC Medical Ethics*, *22*(1). https://doi.org/10.1186/s12910-021-00577-8

Ng, D. T. K., Leung, J. K. L., Chu, S. K. W., & Qiao, M. S. (2021). Conceptualizing AI literacy: An exploratory review. *Computers & Education: Artificial Intelligence*, *2*, 100041. https://doi.org/10.1016/j.caeai.2021.100041

Norberg, P. A., Horne, D. R., & Horne, D. (2007). The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. *˜the œJournal of Consumer Affairs/˜the œJournal of Consumer Affairs*, *41*(1), 100–126. https://doi.org/10.1111/j.1745-6606.2006.00070.x

Oates, B. J. (2005). *Researching information systems and computing*. https://dl.acm.org/citation.cfm?id=1202299

Pan, X., Zhang, M., Ji, S., & Yang, M. (2020). Privacy Risks of General-Purpose Language Models. *2020 IEEE Symposium on Security and Privacy*. https://doi.org/10.1109/sp40000.2020.00095

Park, S., Tung, C. D., & Lee, H. (2021). The adoption of AI service robots: A comparison between credence and experience service settings. *Psychology & Marketing*, *38*(4), 691–703. https://doi.org/10.1002/mar.21468

Perkins, M. (2023). Academic integrity considerations of AI Large Language Models in the post-pandemic era: ChatGPT and beyond. *Journal of University Teaching and Learning Practice*, *20*(2). https://doi.org/10.53761/1.20.02.07

Peterson, R. A., & Kim, Y. (2013). On the relationship between coefficient alpha and composite reliability. *Journal of Applied Psychology*, *98*(1), 194–198. https://doi.org/10.1037/a0030767

Petrosyan, A. (2024, March 27). *Global employees attempting to use ChatGPT at work 2023*. Statista. https://www.statista.com/statistics/1378709/global-employees-chatgpt-se/

Pitardi, V., & Marriott, H. R. (2021). Alexa, she's not human but. . . Unveiling the drivers of consumers' trust in voice-based artificial intelligence. *Psychology & Marketing*, *38*(4), 626–642. https://doi.org/10.1002/mar.21457

Raman, R., Мандал, C., Das, P., Kaur, T., Jp, S., & Nedungadi, P. (2023). University students as early adopters of ChatGPT: Innovation Diffusion Study. *Research Square (Research Square)*. https://doi.org/10.21203/rs.3.rs-2734142/v1

Robinson, P. (2012). Abilities to learn: cognitive abilities. In *Springer eBooks* (pp. 17–20). https://doi.org/10.1007/978-1-4419-1428-6_620

Rueda, M. M., Fernández-Cerero, J., Batanero, J. M. F., & López-Meneses, E. (2023). Impact of the implementation of CHATGPT in Education: A Systematic review. *Computers*, *12*(8), 153. https://doi.org/10.3390/computers12080153

Samoili, S., Montserrat, L. C., Emilia, G. G., Giuditta, D. P., Martínez-Plumed, F., & Delipetrev, B. (2020). AI WATCH. Defining Artificial Intelligence. In *JRC TECHNICAL REPORTS*. Publications Office of the European Union, 2020. https://doi.org/10.2760/382730

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information Privacy: Measuring Individuals' Concerns about Organizational Practices. *Management Information Systems Quarterly*, *20*(2), 167. https://doi.org/10.2307/249477

Steinbauer, G., Kandlhofer, M., Chklovski, T., Heintz, F., & Koenig, S. (2021). A differentiated discussion about AI Education K-12. *KI - Künstliche Intelligenz*, *35*(2), 131–137. https://doi.org/10.1007/s13218-021-00724-8

Su, J., Ng, D. T. K., & Chu, S. K. W. (2023). Artificial intelligence (AI) literacy in Early Childhood education: the challenges and opportunities. *Computers and Education. Artificial Intelligence*, *4*, 100124. https://doi.org/10.1016/j.caeai.2023.100124

Sun, R., Zhu, Q., Cheng, R. X., Tang, W., Zuo, J., Lv, D., & Qin, S. (2024). Research on the cognitive neural mechanism of privacy empowerment illusion cues regarding comprehensibility and interpretability for privacy disclosures. *Scientific Reports*, *14*(1). https://doi.org/10.1038/s41598-024-58917-8

Surfspot. (n.d.). *IBM SPSS - Studenten onderwijskorting*. Retrieved January 15, 2024, from https://www.surfspot.nl/spss

Taherdoost, H. (2016). Sampling methods in research methodology; How to choose a sampling technique for research. *Social Science Research Network*. https://doi.org/10.2139/ssrn.3205035

Tamkin, A., Brundage, M., Clark, J., & Ganguli, D. (2021). Understanding the capabilities, limitations, and societal impact of large language models. *arXiv (Cornell University)*. https://arxiv.org/pdf/2102.02503.pdf

Tiwari, C., Bhat, M. A., Khan, S. T., Subramaniam, R., & Khan, M. A. (2023). What drives students toward ChatGPT? An investigation of the factors influencing adoption and usage of ChatGPT. *Interactive Technology and Smart Education*. https://doi.org/10.1108/itse-04-2023-0061

Vázquez-Cano, E., Ramírez-Hurtado, J. M., Sáez-López, J., & López-Meneses, E. (2023). ChatGPT: The brightest student in the class. *Thinking Skills and Creativity*, *49*, 101380. https://doi.org/10.1016/j.tsc.2023.101380

Xu, H., Dinev, T., Smith, H. J., & Hart, P. (2011). Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances. *Journal of the Association for Information Systems*, *12*(12), 798–824. https://doi.org/10.17705/1jais.00281

Yuan, C. W., Bi, N., Lin, Y., & Tseng, Y. (2023). Contextualizing User Perceptions about Biases for Human-Centered Explainable Artificial Intelligence. *Proceedings of the 2023 CHI Con-Ference on Human Factors in Computing Systems (CHI '23)*. https://doi.org/10.1145/3544548.3580945

Zhou, T. (2011). The impact of privacy concern on user adoption of location-based services. *Industrial Management and Data Systems*, *111*(2), 212–226. https://doi.org/10.1108/02635571111115146

Appendix 1.

MA Thesis AI literacy and privacy

Survey Flow

Standard: Welcome (2 Questions)
Standard: LLM demographic (3 Questions)
Standard: Awareness of privacy practices - Privacy concerns (1 Question)
Standard: Control - Privacy concerns (1 Question)
Standard: Collection - Privacy concerns (1 Question)
Standard: Risk beliefs (1 Question)
Standard: Technical understanding - AI literacy (1 Question)
Standard: Critical Appraisal - AI literacy (1 Question)
Standard: Practical application - AI literacy (1 Question)
Standard: Attitude AI (1 Question)
Standard: Critical thinking (1 Question)
Standard: Demographics (5 Questions)

Page Break

Start of Block: Welcome

Intro **Thank you for your interest in this research.** I am inviting you to fill in a questionnaire. In this questionnaire, there will be questions about what you think about large language models. The purpose of this study is to investigate people's perceptions of large language models and their AI literacy.

The questionnaire will take approximately 10 minutes to fill in. Please answer each question carefully and honestly, I am sincerely interested in your personal opinions. There are no right or wrong answers.

CONFIDENTIALITY OF DATA
All research data remain completely confidential and are collected in anonymous form. We will not be able to identify you. There are no foreseeable risks or discomforts associated with participating in this research.

VOLUNTARY
If you now decide not to participate in this research, this will not affect you. If you decide to cease your cooperation while filling in the questionnaire, this will in no way affect you either. You can cease your cooperation without giving reasons.

FURTHER INFORMATION
If you have questions about this research, in advance or afterwards, you can contact the responsible researcher email: 625815ls@eur.nl. This study has been approved by the Ethics Committee of Erasmus University Rotterdam. If you want to invoke your rights or if you have a question concerning privacy about this study, you can contact Erasmus University's DPO (Data Protection Officer) at fg@eur.nl.

PS: SurveyCircle.com users receive SurveyCircle-points for their participation

Page Break

Consent If you are 18+ years and understand the information above and freely consent to participate in this study, click on the “I agree” button below to start the questionnaire.

- ○ I agree (1)
- ○ I do not agree (2)

Skip To: End of Survey If If you are 18+ years and understand the information above and freely consent to participate in th... = I do not agree

Skip To: End of Block If If you are 18+ years and understand the information above and freely consent to participate in th... = I agree

End of Block: Welcome

Start of Block: LLM demographic

definition Large language models refer to advanced AI systems that are trained to understand and generate human language. People can utilize these models for example for quick and efficient access to domain-specific information, assistance with literature review, text generation support, language translation, and automated summarization etc. For example: you can think of OpenAI's ChatGPT (Generative Pre-trained Transformer) series and Google's BERT (Bidirectional Encoder Representations from Transformers) or similar alternatives.

USAGE Have you ever used any large language model, such as ChatGPT or similar alternatives, to help you in any type of way?

- ○ Yes (1)
- ○ No (2)

Page Break

USAGE_FREQUENCY How often do/did you use large language models, such as ChatGPT or similar alternatives, to help you in any type of way?

- ○ Never (1)
- ○ Once a month (2)
- ○ Several times a month (3)
- ○ Once a week (4)
- ○ Several times a week (5)
- ○ Once a day (6)
- ○ Several times a day (7)
- ○ Once an hour (8)
- ○ Several times an hour (9)
- ○ All the time (10)

End of Block: LLM demographic

Start of Block: Awareness of privacy practices - Privacy concerns

AWARENESS To what extent do you agree with the following statements:

	Strongly agree (1)	Agree (2)	Somewhat agree (3)	Neither agree nor disagree (4)	Somewhat disagree (5)	Disagree (6)	Strongly disagree (7)
Large language models seeking information online should disclose the way the data are collected, processed, and used. (1)	○	○	○	○	○	○	○
A good consumer online privacy policy should have a clear and conspicuous disclosure. (2)	○	○	○	○	○	○	○
It is very important to me that I am aware and knowledgeable about how my personal information will be used. (3)	○	○	○	○	○	○	○

End of Block: Awareness of privacy practices - Privacy concerns

Start of Block: Control - Privacy concerns

CONTROL To what extent do you agree with the following statement:

	Strongly agree (1)	Agree (2)	Somewhat agree (3)	Neither agree nor disagree (4)	Somewhat disagree (5)	Disagree (6)	Strongly disagree (7)
Consumer online privacy is really a matter of consumers' right to exercise control and autonomy over decisions about how their information is collected, used, and shared. (1)	○	○	○	○	○	○	○
Consumer control of personal information lies at the heart of consumer privacy. (2)	○	○	○	○	○	○	○
I believe that online privacy is invaded when control is lost or unwillingly reduced as a result of a marketing transaction. (3)	○	○	○	○	○	○	○

End of Block: Control - Privacy concerns

Start of Block: Collection - Privacy concerns

COLLECTION To what extent do you agree with the following statement:

	Strongly agree (1)	Agree (2)	Somewhat agree (3)	Neither agree nor disagree (4)	Somewhat disagree (5)	Disagree (6)	Strongly disagree (7)
It usually bothers me when large language model companies ask me for personal information. (1)	○	○	○	○	○	○	○
When large language model companies ask me for personal information, I sometimes think twice before providing it. (2)	○	○	○	○	○	○	○
It bothers me to give personal information to a large language model company. (3)	○	○	○	○	○	○	○
I'm concerned that large language models are collecting too much personal information about me. (4)	○	○	○	○	○	○	○

End of Block: Collection - Privacy concerns

Start of Block: Risk beliefs

RISKBELIEFS You are visiting a website of a large language model. The website offers quick and efficient access to domain-specific information, assistance with literature review, text generation support, language translation, and automated summarization to its members.Generally, an annual membership fee is $50. To obtain free membership, you are required to fill out a list about your personal information (e.g., name, surname, adress, email,

phone number, age, purchase preferences, annual income, debt etc.). To what extent do you agree with the following statements:

	Strongly agree (1)	Agree (2)	Somewhat agree (3)	Neither agree nor disagree (4)	Somewhat disagree (5)	Disagree (6)	Strongly disagree (7)
In general, it would be risky to give the information to large language model companies. (1)	○	○	○	○	○	○	○
There would be high potential for loss associated with giving the information to large language model companies. (2)	○	○	○	○	○	○	○
There would be too much uncertainty associated with giving the information to large language model companies. (3)	○	○	○	○	○	○	○
Providing large language model companies with the information would involve many unexpected problems. (4)	○	○	○	○	○	○	○

End of Block: Risk beliefs

Start of Block: Technical understanding - AI literacy

AI TECHNICALUNDERST To what extent do you agree with the following statement: I can...

	Strongly agree (1)	Agree (2)	Somewhat agree (3)	Neither agree nor disagree (4)	Somewhat disagree (5)	Disagree (6)	Strongly disagree (7)
describe how machine learning models are trained, validated and tested (1)	○	○	○	○	○	○	○
explain how deep learning relates to machine learning (2)	○	○	○	○	○	○	○
explain how rule-based systems differ from machine learning systems (3)	○	○	○	○	○	○	○
explain how AI applications make decisions (4)	○	○	○	○	○	○	○
explain how "reinforcement learning" works on a basic level (in the context of machine learning) (5)	○	○	○	○	○	○	○
explain the difference between general (or strong) and narrow (or weak) artificial intelligence (6)	○	○	○	○	○	○	○
explain how sensors are used by computers to collect data that can be used for AI purposes (7)	○	○	○	○	○	○	○
explain what the term "artificial neural network" means (8)	○	○	○	○	○	○	○

explain how machine learning works at a general level (9)	○	○	○	○	○	○	○
explain the difference between "supervised learning" and "unsupervised learning" (in the context of machine learning) (10)	○	○	○	○	○	○	○
describe the concept of explainable AI (11)	○	○	○	○	○	○	○
describe how some artificial intelligence systems can act in their environment and react to their environment (12)	○	○	○	○	○	○	○
describe the concept of big data (13)	○	○	○	○	○	○	○
evaluate wheter media representations of AI (e.g. in movies or video games) go beyond the current capabilities of AI technologies (14)	○	○	○	○	○	○	○

Page Break

End of Block: Technical understanding - AI literacy

Start of Block: Critical Appraisal - AI literacy


AI CRITICALAPPRAISA To what extent do you agree with the following statement: I can...

	Strongly agree (1)	Agree (2)	Somewhat agree (3)	Neither agree nor disagree (4)	Somewhat disagree (5)	Disagree (6)	Strongly disagree (7)
explain why data privacy must be considered when developing and using artificial intelligence applications (1)	○	○	○	○	○	○	○
explain why data security must be considered when developing and using artificial intelligence applications (2)	○	○	○	○	○	○	○
identify ehtical issues surrounding artificial intelligence (3)	○	○	○	○	○	○	○
describe risks that may arise when using artificial intellingence systems (4)	○	○	○	○	○	○	○
name weaknesses of artificial intelligence (5)	○	○	○	○	○	○	○
describe potential legal problems that may arise when using artificial intelligence (6)	○	○	○	○	○	○	○
critically reflect on the potential impact of artificial intelligence on individuals and society (7)	○	○	○	○	○	○	○

describe why humans play an important role in the development of artificial intelligence systems (8)	○	○	○	○	○	○	○
explain why data plays an important role in the development and application of artificial intelligence (9)	○	○	○	○	○	○	○
describe what artificial intelligence is (10)	○	○	○	○	○	○	○

End of Block: Critical Appraisal - AI literacy

Start of Block: Practical application - AI literacy

AI PRACTICALAPPLICA To what extent do you agree with the following statement: I can...

	Strongly agree (1)	Agree (2)	Somewhat agree (3)	Neither agree nor disagree (4)	Somewhat disagree (5)	Disagree (6)	Strongly disagree (7)
give examples from my daily life (personal or professional) where I might be in contact with artificial intelligence (1)	○	○	○	○	○	○	○
name examples of technical applications that are supported by artificial intelligence (2)	○	○	○	○	○	○	○
tell if the technologies I use are supported by artificial intelligence (3)	○	○	○	○	○	○	○
assess if a problem in my field can and should be solved with artificial intelligence methods (4)	○	○	○	○	○	○	○
name applications in which AI-assisted natural language processing/ understanding is used (5)	○	○	○	○	○	○	○
explain why AI has recently become increasingly important (6)	○	○	○	○	○	○	○
critically evaluate the implications of artificial intelligence applications in at least one subject area (7)	○	○	○	○	○	○	○

End of Block: Practical application - AI literacy

Start of Block: Attitude AI

ATTITUDE To what extent do you agree with the following statement:

	Strongly agree (1)	Agree (2)	Somewhat agree (3)	Neither agree nor disagree (4)	Somewhat disagree (5)	Disagree (6)	Strongly disagree (7)
I believe that large language models will improve my life. (1)	○	○	○	○	○	○	○
I believe that large language models will improve my work. (2)	○	○	○	○	○	○	○
I think I will use large language model technology in the future. (3)	○	○	○	○	○	○	○
I think large language model technology is a threat to humans (4)	○	○	○	○	○	○	○

End of Block: Attitude AI

Start of Block: Critical thinking

CRITICAL THINKING

To what extent do you agree with the following statement:

	Strongly agree (1)	Agree (2)	Somewhat agree (3)	Neither agree nor disagree (4)	Somewhat disagree (5)	Disagree (6)	Strongly disagree (7)
I am good at preparing regular plans regarding the solution of the complex problems. (1)	○	○	○	○	○	○	○
It is fun to try to solve the complex problems. (2)	○	○	○	○	○	○	○
I am willing to learn challenging things. (3)	○	○	○	○	○	○	○
I am proud of being able to think with a great precision. (4)	○	○	○	○	○	○	○
I make use of a systematic method while comparing the options at my hand and while reaching a descision (5)	○	○	○	○	○	○	○

End of Block: Critical thinking

Start of Block: Demographics

EDUCATIONLEVEL These are the last questions of the survey! Please don't forget to click the next page button to record your response.

What is the highest level of education you have completed?

- ○ Elementary/ middle school (1)
- ○ High school (2)
- ○ Bachelor's degree (3)
- ○ Master's degree (4)
- ○ PhD (5)

GENDER How would you describe yourself?

- ○ Male (1)
- ○ Female (2)
- ○ Other (3)
- ○ Prefer not to say (4)

NATIONALITY What nationality are you?

▼ Afghan (1) ... Zimbabwean (222)

AGE How old are you?

_____

OCCUPTATION What is your current occupation? (If you are still studying, please write down student)

- ○ Student (1)
- ○ Employed (Full-time) (2)
- ○ Employed (Part-time) (3)
- ○ Self-employed (4)
- ○ Unemployed (5)
- ○ Retired (6)
- ○ Homemaker (7)
- ○ Freelancer/Contractor (8)
- ○ Entrepreneur (9)
- ○ Other (please specify) (10)

_____

End of Block: Demographics

Appendix 2.

Confirmatory factor analysis – Privacy Concerns

Pattern Matrix[a]

	Component		
	1	2	3
To what extent do you agree with the following statement: - Consumer control of personal information lies at the heart of consumer privacy.	.879		
To what extent do you agree with the following statement: - I believe that online privacy is invaded when control is lost or unwillingly reduced as a result of a marketing transaction.	.806		
To what extent do you agree with the following statement: - Consumer online privacy is really a matter of consumers' right to exercise control and autonomy over decisions about how their information is collected, used, and shared.	.611		
To what extent do you agree with the following statement: - It bothers me to give personal information to a large language model company.		-.949	
To what extent do you agree with the following statement: - It usually bothers me when large language model companies ask me for personal information.		-.863	
To what extent do you agree with the following statement: - When large language model companies ask me for personal information, I sometimes think twice before providing it.		-.825	
To what extent do you agree with the following statement: - I'm concerned that large language models are collecting too much personal information about me.		-.775	
To what extent do you agree with the following statements: - Large language models seeking information online should disclose the way the data are collected, processed, and used.			.921
To what extent do you agree with the following statements: - A good consumer online privacy policy should have a clear and conspicuous disclosure.			.725
To what extent do you agree with the following statements: - It is very important to me that I am aware and knowledgeable about how my personal information will be used.			.510

Extraction Method: Principal Component Analysis.
Rotation Method: Oblimin with Kaiser Normalization.

a. Rotation converged in 10 iterations.

Total Variance Explained

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings[a]
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total
1	4.375	43.750	43.750	4.375	43.750	43.750	2.947
2	1.804	18.035	61.785	1.804	18.035	61.785	3.543
3	.829	8.291	70.076	.829	8.291	70.076	2.770
4	.711	7.110	77.186				
5	.530	5.303	82.489				
6	.482	4.815	87.304				
7	.427	4.270	91.574				
8	.374	3.742	95.316				
9	.303	3.026	98.341				
10	.166	1.659	100.000				

Extraction Method: Principal Component Analysis.

a. When components are correlated, sums of squared loadings cannot be added to obtain a total variance.

KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.827
Bartlett's Test of Sphericity	Approx. Chi-Square	697.347
	df	45
	Sig.	<.001

All items load perfectly onto the expected factors Control, Awareness and Collection

Overall reliability: Cronbach's alpha would only get lower if items are deleted.

Reliability Statistics

Cronbach's Alpha	N of Items
.853	10

Awareness: Cronbach's alpha would only get lower if items are deleted.

Reliability Statistics

Cronbach's Alpha	N of Items
.711	3

Control: Cronbach's alpha would only get lower if items are deleted.

Reliability Statistics

Cronbach's Alpha	N of Items
.751	3

Collection: Cronbach's alpha would only get lower if items are deleted.

Reliability Statistics

Cronbach's Alpha	N of Items
.882	4

Confirmatory factor analysis – Risk beliefs

Component Matrix[a]

	Component 1
Think of the scenario you just read, to what extent do you agree with the following statements: - There would be too much uncertainty associated with giving the information to large language model companies.	.894
Think of the scenario you just read, to what extent do you agree with the following statements: - In general, it would be risky to give the information to large language model companies.	.868
Think of the scenario you just read, to what extent do you agree with the following statements: - There would be high potential for loss associated with giving the information to large language model companies.	.864
Think of the scenario you just read, to what extent do you agree with the following statements: - Providing large language model companies with the information would involve many unexpected problems.	.836

Extraction Method: Principal Component Analysis.

a. 1 components extracted.

KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.818
Bartlett's Test of Sphericity	Approx. Chi-Square	348.128
	df	6
	Sig.	<.001

Total Variance Explained

	Initial Eigenvalues			Extraction Sums of Squared Loadings		
Component	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	2.998	74.955	74.955	2.998	74.955	74.955
2	.444	11.091	86.046			
3	.323	8.085	94.131			
4	.235	5.869	100.000			

Extraction Method: Principal Component Analysis.

Cronbach's alpha will only get lower if items are deleted.

Reliability Statistics

Cronbach's Alpha	N of Items
.888	4

Confirmatory factor analysis – Attitude

Component Matrix[a]

	Component 1
To what extent do you agree with the following statement: - I believe that large language models will improve my work.	.900
To what extent do you agree with the following statement: - I think I will use large language model technology in the future.	.862
To what extent do you agree with the following statement: - I believe that large language models will improve my life.	.858
To what extent do you agree with the following statement: - I think large language model technology is a threat to humans	.304

Extraction Method: Principal Component Analysis.

Total Variance Explained

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	2.380	59.510	59.510	2.380	59.510	59.510
2	.971	24.265	83.775			
3	.402	10.056	93.832			
4	.247	6.168	100.000			

Extraction Method: Principal Component Analysis.

KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.699
Bartlett's Test of Sphericity	Approx. Chi-Square	223.599
	df	6
	Sig.	<.001

Reliability Statistics

Cronbach's Alpha	N of Items
.703	4

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
To what extent do you agree with the following statement: - I believe that large language models will improve my life.	8.72	7.386	.660	.530
To what extent do you agree with the following statement: - I believe that large language models will improve my work.	9.05	7.790	.643	.549
To what extent do you agree with the following statement: - I think I will use large language model technology in the future.	9.46	8.393	.597	.586
To what extent do you agree with the following statement: - I think large language model technology is a threat to humans	7.25	9.355	.186	.852

Confirmatory factor analysis – AI literacy

Pattern Matrix[a]

	Component 1	2	3
To what extent do you agree with the following statement: I can... – explain how "reinforcement learning" works on a basic level (in the context of machine learning)	.892		
To what extent do you agree with the following statement: I can... – explain how deep learning relates to machine learning	.866		
To what extent do you agree with the following statement: I can... – explain the difference between general (or strong) and narrow (or weak) artificial intelligence	.851		
To what extent do you agree with the following statement: I can... – explain how rule-based systems differ from machine learning systems	.831		
To what extent do you agree with the following statement: I can... – explain how AI applications make decisions	.819		
To what extent do you agree with the following statement: I can... – describe how some artificial intelligence systems can act in their environment and react to their environment	.812		
To what extent do you agree with the following statement: I can... – describe how machine learning models are trained, validated and tested	.792		
To what extent do you agree with the following statement: I can... – explain how sensors are used by computers to collect data that can be used for AI purposes	.788		
To what extent do you agree with the following statement: I can... – explain how machine learning works at a general level	.780		
To what extent do you agree with the following statement: I can... – explain what the term "artificial neural network" means	.777		
To what extent do you agree with the following statement: I can... – explain the difference between "supervised learning" and "unsupervised learning" (in the context of machine learning)	.735		
To what extent do you agree with the following statement: I can... – describe the concept of explainable AI	.729		
To what extent do you agree with the following statement: I can evaluate whether media representations of AI (e.g., in newspapers or video games) go beyond the current capabilities of AI technologies	.591		
To what extent do you agree with the following statement: I can... – describe the concept of big data	.555		
To what extent do you agree with the following statement: I can... – explain why data security must be considered when developing and using artificial intelligence applications		.886	
To what extent do you agree with the following statement: I can... – explain why data privacy must be considered when developing and using artificial intelligence applications		.878	
To what extent do you agree with the following statement: I can... – identify ethical issues surrounding artificial intelligence		.829	
To what extent do you agree with the following statement: I can... – describe risks that may arise when using artificial intelligence systems		.780	
To what extent do you agree with the following statement: I can... – critically reflect on the potential impact of artificial intelligence on individuals and society		.740	
To what extent do you agree with the following statement: I can... – describe potential legal problems that may arise when using artificial intelligence		.700	
To what extent do you agree with the following statement: I can... – explain why data plays an important role in the development and application of artificial intelligence		.607	
To what extent do you agree with the following statement: I can... – name weaknesses of artificial intelligence		.600	
To what extent do you agree with the following statement: I can... – describe why humans play an important role in the development of artificial intelligence systems		.583	
To what extent do you agree with the following statement: I can... – describe what artificial intelligence is		.444	.394
To what extent do you agree with the following statement: I can... – name examples of technical applications that are supported by artificial intelligence			.876
To what extent do you agree with the following statement: I can... – name applications in which AI-assisted natural language processing/understanding is used			.781
To what extent do you agree with the following statement: I can... – give examples from my daily life (personal or professional) where I might be in contact with artificial intelligence			.768
To what extent do you agree with the following statement: I can... – tell if the technologies I use are supported by artificial intelligence			.760
To what extent do you agree with the following statement: I can... – explain why AI has recently become increasingly important			.686
To what extent do you agree with the following statement: I can... – assess if a problem in my field can and should be solved with artificial intelligence methods			.639
To what extent do you agree with the following statement: I can... – critically evaluate the implications of artificial intelligence applications in at least one subject area			.633

Extraction Method: Principal Component Analysis.
Rotation Method: Oblimin with Kaiser Normalization.[a]

a. Rotation converged in 7 iterations.

Total Variance Explained

Component	Initial Eigenvalues Total	% of Variance	Cumulative %	Extraction Sums of Squared Loadings Total	% of Variance	Cumulative %	Rotation Sums of Squared Loadings[a] Total
1	12.173	39.268	39.268	12.173	39.268	39.268	10.027
2	5.112	16.492	55.760	5.112	16.492	55.760	8.285
3	1.958	6.317	62.077	1.958	6.317	62.077	7.509
4	1.024	3.302	65.380				
5	.933	3.008	68.388				
6	.826	2.665	71.053				
7	.823	2.653	73.706				
8	.734	2.368	76.075				

KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.920
Bartlett's Test of Sphericity	Approx. Chi-Square	3551.515
	df	465
	Sig.	.000

technical understanding:

Reliability Statistics

Cronbach's Alpha	N of Items
.953	14

critical appraisal:

Reliability Statistics

Cronbach's Alpha	N of Items
.921	10

practical application:

Reliability Statistics

Cronbach's Alpha	N of Items
.881	7

Deleting any items would not increasy reliability.

Confirmatory Factor Analysis – Critical thinking

Component Matrix[a]

	Component 1
To what extent do you agree with the following statement: - I am willing to learn challenging things.	.851
To what extent do you agree with the following statement: - It is fun to try to solve the complex problems.	.835
To what extent do you agree with the following statement: - I am proud of being able to think with a great precision.	.751
To what extent do you agree with the following statement: - I make use of a systematic method while comparing the options at my hand and while reaching a descision	.691
To what extent do you agree with the following statement: - I am good at preparing regular plans regarding the solution of the complex problems.	.554

Extraction Method: Principal Component Analysis.

a. 1 components extracted.

KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.768
Bartlett's Test of Sphericity	Approx. Chi-Square	248.846
	df	10
	Sig.	<.001

Total Variance Explained

	Initial Eigenvalues			Extraction Sums of Squared Loadings		
Component	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	2.768	55.368	55.368	2.768	55.368	55.368
2	.801	16.022	71.390			
3	.656	13.126	84.516			
4	.517	10.343	94.859			
5	.257	5.141	100.000			

Extraction Method: Principal Component Analysis.

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
To what extent do you agree with the following statement: - I am good at preparing regular plans regarding the solution of the complex problems.	10.10	13.465	.392	.807
To what extent do you agree with the following statement: - It is fun to try to solve the complex problems.	10.28	11.010	.682	.714
To what extent do you agree with the following statement: - I am willing to learn challenging things.	10.60	11.397	.701	.710
To what extent do you agree with the following statement: - I am proud of being able to think with a great precision.	10.48	12.355	.579	.750
To what extent do you agree with the following statement: - I make use of a systematic method while comparing the options at my hand and while reaching a descision	10.20	12.369	.516	.770

Reliability Statistics

Cronbach's Alpha	N of Items
.792	5

Cronbach's alpha can increase to **.807** if "I am good at preparing regular plans regarding the solution of the complex problems" is deleted.

But it does not increase at least .05 so it will not be deleted.

Regression analysis

H1: Privacy concerns are positively associated with the risk beliefs of users towards large language models.

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics			
					R Square Change	F Change	df1	df2	Sig. F Change
1	.545[a]	.297	.292	.98935	.297	64.658	1	153	<.001

a. Predictors: (Constant), PrivacyConcern

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	63.288	1	63.288	64.658	<.001[b]
	Residual	149.758	153	.979		
	Total	213.046	154			

a. Dependent Variable: Risk

b. Predictors: (Constant), PrivacyConcern

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	1.185	.237		5.009	<.001
	PrivacyConcern	.783	.097	.545	8.041	<.001

a. Dependent Variable: Risk

Regression analysis

H2: Privacy concerns are negatively associated with users' attitude toward large language models.

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics			
					R Square Change	F Change	df1	df2	Sig. F Change
1	.157[a]	.025	.018	1.01012	.025	3.884	1	153	.051

a. Predictors: (Constant), PrivacyConcern

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	3.963	1	3.963	3.884	.051[b]
	Residual	156.113	153	1.020		
	Total	160.076	154			

a. Dependent Variable: Attitude

b. Predictors: (Constant), PrivacyConcern

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	2.863	.242		11.853	<.001
	PrivacyConcern	-.196	.099	-.157	-1.971	.051

a. Dependent Variable: Attitude

Regression analysis PROCESS
Moderation privacy concerns – risk beliefs – AI literacy technical understanding

Run MATRIX procedure:

***************** PROCESS Procedure for SPSS Version 4.2 *****************

Written by Andrew F. Hayes, Ph.D. www.afhayes.com
Documentation available in Hayes (2022). www.guilford.com/p/hayes3

****
Model : 1
Y : Risk
X : PrivCon
W : LitTecUn

Sample
Size: 155

****
OUTCOME VARIABLE:
Risk

Model Summary

R	R-sq	MSE	F	df1	df2	p
.5659	.3203	.9590	23.7184	3.0000	151.0000	.0000

Model

	coeff	se	t	p	LLCI	ULCI
constant	.9716	.6760	1.4373	.1527	-.3641	2.3073
PrivCon	1.0891	.2821	3.8604	.0002	.5317	1.6466
LitTecUn	.0586	.1434	.4088	.6833	-.2246	.3418
Int_1	-.0751	.0614	-1.2226	.2234	-.1964	.0463

Product terms key:
Int_1 : PrivCon x LitTecUn

Test(s) of highest order unconditional interaction(s):

	R2-chng	F	df1	df2	p
X*W	.0067	1.4946	1.0000	151.0000	.2234

********************** ANALYSIS NOTES AND ERRORS ************************

Level of confidence for all confidence intervals in output:
95.0000

------ END MATRIX -----

Moderation privacy concerns – risk beliefs – AI literacy critical appraisal

Run MATRIX procedure:

```
***************** PROCESS Procedure for SPSS Version 4.2 *****************

        Written by Andrew F. Hayes, Ph.D.       www.afhayes.com
    Documentation available in Hayes (2022). www.guilford.com/p/hayes3

**************************************************************************
Model  : 1
    Y  : Risk
    X  : PrivCon
    W  : LitCriAp

Sample
Size:  155

**************************************************************************
OUTCOME VARIABLE:
 Risk

Model Summary
        R       R-sq        MSE          F        df1        df2          p
     .5501      .3026      .9839    21.8438     3.0000   151.0000      .0000

Model
            coeff         se          t          p       LLCI       ULCI
constant    1.2016      .5679     2.1160      .0360      .0796     2.3236
PrivCon      .8827      .2601     3.3935      .0009      .3688     1.3966
LitCriAp    -.0192      .1879     -.1020      .9189     -.3905      .3521
Int_1       -.0296      .0839     -.3528      .7247     -.1954      .1362

Product terms key:
 Int_1    :       PrivCon  x       LitCriAp

Test(s) of highest order unconditional interaction(s):
      R2-chng          F        df1        df2          p
X*W      .0006      .1245     1.0000   151.0000      .7247

************************ ANALYSIS NOTES AND ERRORS ************************

Level of confidence for all confidence intervals in output:
  95.0000

------ END MATRIX -----
```

Moderation privacy concerns – risk beliefs – AI literacy Practical application

Run MATRIX procedure:

```
***************** PROCESS Procedure for SPSS Version 4.2 *****************

        Written by Andrew F. Hayes, Ph.D.       www.afhayes.com
    Documentation available in Hayes (2022). www.guilford.com/p/hayes3

**************************************************************************
Model  : 1
    Y  : Risk
    X  : PrivCon
    W  : LitPraAp

Sample
Size:  155

**************************************************************************
OUTCOME VARIABLE:
 Risk

Model Summary
        R       R-sq        MSE          F        df1        df2          p
     .5493      .3018      .9851    21.7551     3.0000   151.0000      .0000

Model
            coeff         se          t          p       LLCI       ULCI
constant   1.7248     .6073     2.8401     .0051     .5249     2.9247
PrivCon     .5975     .2571     2.3241     .0215     .0895     1.1054
LitPraAp   -.2035     .2117    -.9611     .3381    -.6218     .2148
Int_1       .0701     .0910     .7696     .4427    -.1098     .2499

Product terms key:
 Int_1    :       PrivCon  x       LitPraAp

Test(s) of highest order unconditional interaction(s):
      R2-chng          F        df1        df2          p
X*W      .0027      .5923     1.0000   151.0000      .4427

************************ ANALYSIS NOTES AND ERRORS
************************

Level of confidence for all confidence intervals in output:
  95.0000

------ END MATRIX -----
```

Moderation privacy concerns – attitude – AI literacy technical understanding

Run MATRIX procedure:

```
***************** PROCESS Procedure for SPSS Version 4.2 *****************

        Written by Andrew F. Hayes, Ph.D.       www.afhayes.com
    Documentation available in Hayes (2022). www.guilford.com/p/hayes3

**************************************************************************
Model  : 1
    Y  : Attitude
    X  : PrivCon
    W  : LitTecUn

Sample
Size:  155

**************************************************************************
OUTCOME VARIABLE:
 Attitude

Model Summary
        R       R-sq        MSE          F        df1        df2          p
     .2031      .0412     1.0164     2.1648     3.0000   151.0000      .0945

Model
            coeff         se          t          p       LLCI       ULCI
constant   2.0640     .6960     2.9657     .0035     .6889     3.4391
PrivCon     .0068     .2905     .0236      .9812    -.5670     .5807
LitTecUn    .1757     .1476     1.1905     .2357    -.1159     .4673
Int_1      -.0438     .0632    -.6923      .4898    -.1687     .0812

Product terms key:
 Int_1    :       PrivCon  x       LitTecUn

Test(s) of highest order unconditional interaction(s):
      R2-chng          F        df1        df2          p
X*W      .0030      .4793     1.0000   151.0000      .4898

************************ ANALYSIS NOTES AND ERRORS ************************

Level of confidence for all confidence intervals in output:
  95.0000

------ END MATRIX -----
```

Moderation privacy concerns – attitude – AI literacy critical appraisal

Run MATRIX procedure:

***************** PROCESS Procedure for SPSS Version 4.2 *****************

Written by Andrew F. Hayes, Ph.D. www.afhayes.com
Documentation available in Hayes (2022). www.guilford.com/p/hayes3

****
Model : 1
Y : Attitude
X : PrivCon
W : LitCriAp

Sample
Size: 155

****
OUTCOME VARIABLE:
Attitude

Model Summary

R	R-sq	MSE	F	df1	df2	p
.3327	.1107	.9428	6.2648	3.0000	151.0000	.0005

Model

	coeff	se	t	p	LLCI	ULCI
constant	3.4935	.5559	6.2847	.0000	2.3952	4.5918
PrivCon	-.8088	.2546	-3.1763	.0018	-1.3118	-.3057
LitCriAp	-.1864	.1840	-1.0131	.3126	-.5499	.1771
Int_1	.1993	.0822	2.4262	.0164	.0370	.3617

Product terms key:
Int_1 : PrivCon x LitCriAp

Test(s) of highest order unconditional interaction(s):

	R2-chng	F	df1	df2	p
X*W	.0347	5.8865	1.0000	151.0000	.0164

Focal predict: PrivCon (X)
Mod var: LitCriAp (W)

Conditional effects of the focal predictor at values of the moderator(s):

LitCriAp	Effect	se	t	p	LLCI	ULCI
1.7170	-.4665	.1351	-3.4521	.0007	-.7335	-.1995
2.7716	-.2563	.0969	-2.6450	.0090	-.4477	-.0648
3.8263	-.0461	.1246	-.3696	.7122	-.2923	.2002

Moderator value(s) defining Johnson-Neyman significance region(s):

Value	% below	% above
3.0840	65.8065	34.1935

Conditional effect of focal predictor at values of the moderator:

LitCriAp	Effect	se	t	p	LLCI	ULCI
1.0000	-.6094	.1813	-3.3614	.0010	-.9676	-.2512
1.2600	-.5576	.1636	-3.4080	.0008	-.8809	-.2343
1.5200	-.5058	.1469	-3.4426	.0007	-.7960	-.2155
1.7800	-.4539	.1316	-3.4503	.0007	-.7139	-.1940
2.0400	-.4021	.1181	-3.4047	.0008	-.6355	-.1688
2.3000	-.3503	.1072	-3.2664	.0013	-.5622	-.1384
2.5600	-.2985	.0998	-2.9899	.0033	-.4957	-.1012
2.8200	-.2466	.0967	-2.5518	.0117	-.4376	-.0557
3.0800	-.1948	.0981	-1.9851	.0489	-.3887	-.0009
3.0840	-.1940	.0982	-1.9758	.0500	-.3880	.0000
3.3400	-.1430	.1041	-1.3738	.1715	-.3486	.0627
3.6000	-.0912	.1138	-.8012	.4243	-.3160	.1337
3.8600	-.0393	.1264	-.3112	.7561	-.2891	.2104
4.1200	.0125	.1411	.0885	.9296	-.2663	.2913
4.3800	.0643	.1574	.4087	.6833	-.2466	.3752
4.6400	.1161	.1747	.6647	.5073	-.2291	.4614
4.9000	.1680	.1929	.8708	.3853	-.2131	.5491
5.1600	.2198	.2117	1.0385	.3007	-.1984	.6380
5.4200	.2716	.2309	1.1765	.2412	-.1845	.7278
5.6800	.3234	.2504	1.2916	.1985	-.1714	.8182
5.9400	.3753	.2703	1.3885	.1670	-.1587	.9093
6.2000	.4271	.2903	1.4712	.1433	-.1465	1.0007

********** ANALYSIS NOTES AND ERRORS **********

Level of confidence for all confidence intervals in output:
95.0000

W values in conditional tables are the mean and +/- SD from the mean.

------ END MATRIX -----

Moderation privacy concerns – attitude – AI literacy practical application

Run MATRIX procedure:

***************** PROCESS Procedure for SPSS Version 4.2 *****************

Written by Andrew F. Hayes, Ph.D. www.afhayes.com
Documentation available in Hayes (2022). www.guilford.com/p/hayes3

****
Model : 1
Y : Attitude
X : PrivCon
W : LitPraAp

Sample
Size: 155

****
OUTCOME VARIABLE:
Attitude

Model Summary

R	R-sq	MSE	F	df1	df2	p
.4583	.2100	.8375	13.3808	3.0000	151.0000	.0000

Model

	coeff	se	t	p	LLCI	ULCI
constant	2.7451	.5599	4.9025	.0000	1.6388	3.8514
PrivCon	-.6429	.2370	-2.7125	.0075	-1.1112	-.1746
LitPraAp	.0294	.1952	.1506	.8805	-.3563	.4151
Int_1	.1786	.0839	2.1280	.0350	.0128	.3445

Product terms key:
Int_1 : PrivCon x LitPraAp

Test(s) of highest order unconditional interaction(s):

	R2-chng	F	df1	df2	p
X*W	.0237	4.5282	1.0000	151.0000	.0350

Focal predict: PrivCon (X)
Mod var: LitPraAp (W)

Conditional effects of the focal predictor at values of the moderator(s):

LitPraAp	Effect	se	t	p	LLCI	ULCI
1.6255	-.3525	.1224	-2.8811	.0045	-.5943	-.1108
2.6175	-.1753	.0901	-1.9455	.0536	-.3534	.0027
3.6095	.0019	.1231	.0150	.9880	-.2413	.2450

Moderator value(s) defining Johnson-Neyman significance region(s):

Value	% below	% above
2.6022	60.6452	39.3548

Conditional effect of focal predictor at values of the moderator:

LitPraAp	Effect	se	t	p	LLCI	ULCI
1.0000	-.4643	.1625	-2.8563	.0049	-.7854	-.1431
1.2500	-.4196	.1455	-2.8830	.0045	-.7072	-.1320
1.5000	-.3750	.1297	-2.8905	.0044	-.6313	-.1187
1.7500	-.3303	.1156	-2.8585	.0049	-.5586	-.1020
2.0000	-.2857	.1037	-2.7541	.0066	-.4906	-.0807
2.2500	-.2410	.0951	-2.5341	.0123	-.4289	-.0531
2.5000	-.1963	.0906	-2.1668	.0318	-.3754	-.0173
2.6022	-.1781	.0901	-1.9758	.0500	-.3562	.0000
2.7500	-.1517	.0909	-1.6691	.0972	-.3312	.0279
3.0000	-.1070	.0958	-1.1166	.2659	-.2964	.0824
3.2500	-.0624	.1049	-.5948	.5529	-.2696	.1448
3.5000	-.0177	.1170	-.1514	.8799	-.2489	.2134
3.7500	.0269	.1314	.2051	.8378	-.2326	.2865
4.0000	.0716	.1473	.4860	.6277	-.2195	.3627
4.2500	.1163	.1644	.7070	.4807	-.2087	.4412
4.5000	.1609	.1824	.8824	.3790	-.1994	.5212
4.7500	.2056	.2009	1.0234	.3078	-.1913	.6024
5.0000	.2502	.2198	1.1383	.2568	-.1841	.6846
5.2500	.2949	.2391	1.2332	.2194	-.1776	.7673
5.5000	.3395	.2587	1.3126	.1913	-.1716	.8506
5.7500	.3842	.2784	1.3798	.1697	-.1660	.9344
6.0000	.4289	.2984	1.4373	.1527	-.1607	1.0184

********** ANALYSIS NOTES AND ERRORS **********

Level of confidence for all confidence intervals in output:
95.0000

W values in conditional tables are the mean and +/- SD from the mean.

------ END MATRIX -----

MEDIATION privacy concerns – risk – critical thinking

Run MATRIX procedure:

***************** PROCESS Procedure for SPSS Version 4.2 *****************

Written by Andrew F. Hayes, Ph.D. www.afhayes.com
Documentation available in Hayes (2022). www.guilford.com/p/hayes3

****
Model : 4
Y : Risk
X : PrivCon
M : CritThin

Sample
Size: 155

****
OUTCOME VARIABLE:
CritThin

Model Summary

R	R-sq	MSE	F	df1	df2	p
.2455	.0603	.6810	9.8159	1.0000	153.0000	.0021

Model

	coeff	se	t	p	LLCI	ULCI
constant	2.0008	.1974	10.1377	.0000	1.6109	2.3907
PrivCon	.2544	.0812	3.1330	.0021	.0940	.4149

****
OUTCOME VARIABLE:
Risk

Model Summary

R	R-sq	MSE	F	df1	df2	p
.5514	.3041	.9754	33.2065	2.0000	152.0000	.0000

Model

	coeff	se	t	p	LLCI	ULCI
constant	.9458	.3054	3.0969	.0023	.3424	1.5492
PrivCon	.7525	.1003	7.5046	.0000	.5544	.9505
CritThin	.1197	.0968	1.2373	.2179	-.0714	.3109

****************** DIRECT AND INDIRECT EFFECTS OF X ON Y
****

Direct effect of X on Y

```
    Effect         se          t          p       LLCI       ULCI
     .7525      .1003     7.5046      .0000      .5544      .9505

Indirect effect(s) of X on Y:
           Effect    BootSE   BootLLCI   BootULCI
CritThin     .0305     .0353     -.0205     .1172

************************ ANALYSIS NOTES AND ERRORS
************************

Level of confidence for all confidence intervals in output:
  95.0000

Number of bootstrap samples for percentile bootstrap confidence intervals:
  5000

------ END MATRIX -----
```

MEDIATION privacy concerns - attitude – critical thinking

```
Run MATRIX procedure:

***************** PROCESS Procedure for SPSS Version 4.2 *****************

        Written by Andrew F. Hayes, Ph.D.       www.afhayes.com
    Documentation available in Hayes (2022). www.guilford.com/p/hayes3

**************************************************************************
Model  : 4
    Y  : Attitude
    X  : PrivCon
    M  : CritThin

Sample
Size:  155

**************************************************************************
OUTCOME VARIABLE:
 CritThin

Model Summary
         R       R-sq        MSE          F        df1        df2          p
     .2455      .0603      .6810     9.8159     1.0000   153.0000      .0021

Model
            coeff         se          t          p       LLCI       ULCI
constant     2.0008      .1974    10.1377      .0000     1.6109     2.3907
```

```
PrivCon      .2544     .0812    3.1330     .0021     .0940     .4149

**************************************************************************
OUTCOME VARIABLE:
 Attitude

Model Summary
        R       R-sq        MSE          F        df1        df2          p
     .3929      .1544      .8906    13.8724     2.0000   152.0000      .0000

Model
             coeff         se          t          p       LLCI       ULCI
constant    1.9707      .2918     6.7532      .0000     1.3942     2.5472
PrivCon     -.3094      .0958    -3.2299      .0015     -.4987     -.1202
CritThin     .4462      .0925     4.8265      .0000      .2636      .6289


****************** DIRECT AND INDIRECT EFFECTS OF X ON Y
*****************

Direct effect of X on Y
    Effect         se          t          p       LLCI       ULCI
    -.3094      .0958    -3.2299      .0015     -.4987     -.1202

Indirect effect(s) of X on Y:
            Effect     BootSE   BootLLCI   BootULCI
CritThin     .1135      .0560      .0160      .2309

************************ ANALYSIS NOTES AND ERRORS
************************

Level of confidence for all confidence intervals in output:
  95.0000

Number of bootstrap samples for percentile bootstrap confidence intervals:
  5000

------ END MATRIX -----
```