Journal of Global Information Management
Volume 33 • Issue 1 • January-December 2025

Artificial Intelligence (AI) and the Future of Information Privacy:
Expert Viewpoints

Alfred Akakpo
https://orcid.org/0000-0003-3014-1173
University of Northampton, UK

Evans Akwasi Gyasi
https://orcid.org/0000-0002-1104-8515
Anglia Ruskin University, UK

Bentil Oduro
https://orcid.org/0009-0003-9422-9411
Coventry University, UK

Sunny Akpabot
Coventry University, UK

ABSTRACT

AI's expanding role in daily life offers data-driven decision-making but risks privacy breaches. This study, using the Communication Privacy Management theory, explores AI adoption's future privacy implications. Through thematic analysis of 42 AI expert interviews, we identify six key themes: human agency, data use/abuse, AI transparency/opacity, information weaponization, cyberbullying, and privacy enforcement. These themes contextualize the evolving AI-privacy relationship. We argue that AI's advancement will challenge traditional privacy ownership concepts. This research provides insights into navigating the complex interplay between AI's growth and safeguarding information privacy

KEYWORDS

Artificial Intelligence, Information Privacy, Privacy Concerns, Communication Privacy Management Theory

INTRODUCTION

Human activities are structured and facilitated by sophisticated communication, information, and technology infrastructures. These advances are reshaping our modes of communication, business operations, and information exchange among friends, families, organizations, and global communities. Artificial intelligence (AI) stands out as a pervasive modern technology holding the vast potential to profoundly transform interactions, lifestyles, and professional engagements (Fogli & Tetteroo, 2022; Jang, 2023; Ku & Chen, 2024; Smilansky, 2017; Wang et al., 2023). However, the immense power of AI technology with access to large and rich data has created concerns about privacy and anonymity.

According to Madakam et al. (2015), AI is a computer-generated technology that uses natural algorithms to perform tasks that may require human intelligence. Recent literature on AI and the future of data protection and privacy has received significant interest within academia and industrial fields (Wu et al., 2019). For example, researchers have probed the implications for the right of privacy

DOI: 10.4018/JGIM.383050

related to the following scenarios: the use of AI technologies to administer justice in courts (Fiechuk, 2019), application of AI in public sector management (Maragno et al., 2023), and integration of AI into smart meter technology (Lodder & Wisman, 2015). Collins et al. (2021) conducted a systematic literature review on AI in information systems research. In addition, Wang et al. (2023) proposed the concept of AI literacy by developing a quantitative scale for measuring the accuracy of AI literacy. They concluded that not only will the scale create an understanding of user competency with AI technology, but it will also assist designers with developing AI applications that will align with the level of AI literacy of target users. Johnson and Verdicchio (2017) explored public anxiety surrounding artificial intelligence, particularly concerning privacy. Their research identified a primary driver of this apprehension: a significant fear that AI systems could soon operate beyond the limits of human control. Also, as pointed out in Johnson and Verdicchio's work, the focus on AI programs without human involvement is flawed because, regardless of advances in AI and superintelligence, there will be a need for human engagement to a considerable extent with such programs. Furthermore, Johnson and Verdicchio argue that the next form of anxiety will emanate from the concept of autonomy, which means the extent to which AI programs would be fully autonomous to make decisions without human intervention. Johnson and Verdicchio(2017) identified that leaving computers to make such decisions without human involvement could impact privacy issues. Importantly, Johnson and Verdicchio (2017) differentiated between computational and human autonomy. Humans have the power to make decisions based on fundamental rights and are well-equipped to understand the context of human decision-making. On the other hand, computational autonomy may not be able to make such judgements in the event of changes in context. Thus, computational autonomy seems to conflict with human autonomy in data protection and privacy. Researchers in AI, such as Müller (2016), have asserted that in a futuristic scenario, robots could behave like humans and may harm others to achieve their objectives.

Prior studies about privacy-related decision making are built on the assumption of a rational process for individuals to disclose information about themselves willingly, with this process being guided by an internal cognitive assessment of perceived risk and perceived benefits associated with the disclosure of personal information (Cai et al., 2023; Culnan & Armstrong, 1999; Degirmenci, 2020; Dinev & Hart, 2006; Park et al., 2023). However, other research casts doubt on the rationality of privacy disclosure and states that rational considerations are guided by heuristics and limited resources (Brandimarte et al., 2013; Tsai et al., 2011). At the same time, a few studies have argued against the urgency and significance of privacy research because there are considerable gaps in the research on how to contextualize and reconceptualize privacy in the digital age, improve organizational practices, and protect the information of individuals and groups (Wu et al., 2019).

Stakeholders need to understand how AI is influencing privacy in the digital age. Indeed, calls have been made to demystify how the adoption of new technology is influencing privacy. We respond to this call and follow prior studies by Acquisti et al. (2015) and Wu et al. (2019) by developing a framework to address the following research questions: What are the future challenges of privacy because of AI adoption, and how can stakeholders address privacy challenges in the age of AI technology? To address the research question, we followed two specific objectives: first, to examine the impact of AI adoption on information privacy; and second, to develop a conceptual framework for measuring the relationship between AI adoption and information privacy concerns.

This article makes four main contributions to the field of AI technology and privacy concerns, thus building on communication privacy management CPM) theory to offer a comprehensive theoretical framework for understanding the adoption of AI and its implications for information privacy. This study is different from earlier studies because it is one of the few to draw on CPM theory to explain AI adoption and information privacy from experts' viewpoints and to argue that with the advance and proliferation of AI technologies, there will be the weaponization of information: that is, private information that was collected by AI technologies without the permission of its owners will be used as weapons to blackmail and subvert individuals.

In addition, this article contributes to the extant literature on AI adoption and privacy by identifying six emerging themes that contextualize the future of AI adoption and information privacy, including human agency, data use and abuse, AI transparency and opacity, weaponization of information, cyberbullying, and privacy issues and enforcement of privacy strategies. These themes provide a framework for analyzing the multifaceted impact of AI on privacy and serve as a basis for future research and policymaking efforts.

Finally, the findings also contribute to the literature by forecasting that as AI adoption expands, there will be a lack of ownership of privacy because individuals, governments and policymakers will resolve and accept the benefits of AI at the expense of information privacy concerns and will see data abuse as a normal practice. This exploratory study on AI and information privacy demonstrates that there is strong anxiety about the future of AI adoption and how to maintain a balance with privacy rights (Johnson & Verdicchio, 2017).

The rest of the paper is structured in the following way. After the introduction section that sets the tone for the study, the following section presents the concept of privacy and background on the relevant theoretical model that underpins this research. This section is followed by a discussion of data collection and the method of data analysis, which involves how information from relevant sources is gathered and analyzed. This section is followed by findings, which present the results and the emerging themes. The final section is the conclusion, which consists of the contribution of the study, the limitations of the study, and future research recommendations.

THE CONCEPT OF PRIVACY

Theories of privacy can be traced back over 50 years and are linked with individuals' rights to decide how information about themselves should be shared with others and the conditions of communicating such information (Steeves, 2019). A traditional concept of privacy that has stood the test of time was proposed by Westin (1968). He defined privacy as the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others (Westin, 1968). This definition by Westin has been explored and expanded on by other authors. For example, information privacy is defined as the desire of individuals to control or have some influence over data about themselves (Bélanger & Crossler, 2011). H. J. Smith et al. (1996) explained information privacy by identifying four dimensions of information privacy: collection, improper access, unauthorized secondary use, and errors. In another study, Solove (2006) considered information privacy to consist of information collection, information dissemination, information processing, and invasion of privacy. Information privacy concerns stem from legal rules aimed at protecting the privacy of people's information to deter unauthorized use of or access to this information. Thus, information privacy is the collection and storage of personal data in a manner that allows individuals to have control and influence over how information and data are handled and used. While privacy is an ingredient cherished by most people, whether absolute privacy can be achieved with the proliferation of technologies such as AI and social media is debatable.

Theoretical Background

This paper draws on CPM theory (Petronio, 1991) to explain how AI will affect information privacy in society. CPM theory was proposed by Petronio (1991, 2004, 2010) and consists of three elements: privacy control, privacy ownership, and privacy turbulence. Privacy control governs the conditions for denying or allowing access to private information. These conditions enable a person to manage personal information even after giving access to others. Privacy control, in conjunction with other elements, develops guidelines and rules driven by decisions and criteria such as cultural values, motivation, and the need for such information (Petronio, 2010). The second element of CPM is privacy ownership, which enables people to envisage that they are the sole owners of their private information and to trust they have the right to grant or prevent access to their information

(Petronio, 2010). Ownership implies the equal right to share or to restrict information and to define boundaries surrounding information that can be marked as private (Thompson et al., 2012). The third element of the CPM model is privacy turbulence; this element helps predict and regulate information privacy that is often unpredictable, with disruptions to a complete privacy management system breakdown. For example, individuals maintain personal privacy boundaries; however, when these boundaries are disrupted, it creates turbulence. Such disruptions prompt individuals to reorganize their privacy boundaries to prevent similar disturbances in the future (Petronio, 2010).

Since the development of the CPM model, several studies have utilised the model. For example, Smith and Brunner (2017) employed CPM to understand how information is disclosed at the workplace. Walrave et al. (2022) utilized CPM to examine how parents disclose information about their children online, while LaBelle et al. (2023) used CPM to understand how graduate students decide to disclose their mental health conditions to their academic advisors. These studies show how widely CPM has been applied in different privacy studies.

This article draws on CPM theory to provide a foundation for future research endeavours by exploring the complex dynamics between AI adoption and information privacy. We posit that AI adoption and information privacy in terms of privacy control, privacy ownership, and privacy turbulence will be determined by data use and abuse, AI transparency and opacity, and weaponization of information in the light of increasing AI adoption. We suggest that researchers can build upon the insights and framework proposed in this study to investigate specific aspects of AI ethics, privacy management, and the implications of AI technologies on society.

Artificial Intelligence Applications in Different Fields

The rapid integration of AI into organizational management has significantly improved efficiency and productivity across various industries. However, the widespread adoption of AI still encounters several obstacles, including ethical concerns, organizational resistance, privacy issues, and a shortage of relevant technological expertise (Hasan et al., 2023). These findings of Hasan et al. (2023) closely align with the discussion of AI's role in financial decision making. While AI has demonstrated its potential to enhance investment strategies and to mitigate behavioural biases among financial planners, its successful adoption depends on overcoming concerns associated with privacy, trust, perceived costs, and anxiety surrounding AI technologies (Maldonado-Canca et al., 2025). By addressing these barriers, AI can be more effectively integrated into financial planning services, allowing professionals to leverage its capabilities to counteract confirmation and hindsight biases.

Rahman et al. (2024) provided empirical evidence of business intelligence's (BI's)role in enhancing operational efficiency and facilitating AI adoption within a specific sector. Also, Bag et al. (2025) offered a broader theoretical framework for understanding AI's impact on social engagement. A key difference lies in their methodologies. Rahman et al. (2024) employed quantitative methods to measure tangible outcomes, whereas Bag et al. (2025) used qualitative and computational approaches to explore broader themes and discourses. This divergence reflects different research questions and objectives of the studies. Both studies could benefit from addressing the ethical and privacy implications of AI. Rahman et al. (2024) could explore the ethical considerations surrounding data privacy and algorithmic bias in financial applications, while Bag et al. (2025) could delve into the challenges of using AI for social engagement, such as the potential for manipulation and misinformation.

After reviewing the existing literature on AI, we have identified a significant gap regarding its impact on information privacy. To address this gap, our study critically examines the perspectives of AI experts on information privacy, offering valuable insights into this often-overlooked area. Table 1 below summarises the key literature on AI and information privacy to legitimise the importance and timeliness of this study.

Table 1. Summary of Key Literature on AI and Information Privacy

	Author	Focus of the study	Method	Field of study
Information Privacy	Agozie & Kaya (2021)	Privacy information transparency and mitigating privacy fatigue	Survey	E-government
	Soumelidou & Tsobou (2024)	Mobile applications and information privacy		Mobile application users
	Attili et al. (2022)	Information privacy in IT organizations	Survey	IT organizations in India and the United States
	Sun et al. (2022)	Social media and information privacy violations		Social media users in China and the United States
Artificial Intelligence	Hasan et al. (2023)	AI and financial planning	Literature review	To propose artificial intelligence to manage behavioural biases in the financial decision-making process in financial institutions
	Rahman et al. (2024)	AI and BI on operational efficiency in the financial sector	Secondary data from Shanghai and Shenzhen	The impact of BI systems on operational efficiency and the transition to artificial intelligence technologies in Shanghai financial firms and Shenzhen stock markets
	Maldonado-Canca et al. (2024)	The adoption of AI by companies enhances the UTAUT model variables.	Survey	409 CEOs and entrepreneurs from various organizations located in Spain
	Bag et al. (2025)	AI and stakeholder engagement in addressing climate change	Systematic literature review	Various sectors

METHODOLOGY

Data and Sample

This study draws upon extensive interviews conducted by the Pew Research Center in December 2018 and June 2023 involving 979 AI experts from diverse backgrounds, including activists, business and policy leaders, developers, innovators, researchers, and technology pioneers. The interviews focused on the theme 'Artificial Intelligence and the Future of Humans.' The Pew Research Center, a nonpartisan think tank dedicated to conducting surveys and informing the public about prevailing attitudes, issues, and trends shaping the United States and the world, facilitated this research. The interview responses are publicly available on the Pew Research Center website (Anderson & Rainie, 2019, 2023). Our study employed a qualitative research approach to analyze AI experts' perspectives on AI adoption and information privacy. This approach allowed us to gather rich, nuanced data that may not have been captured through quantitative methods.

Data Collection

To explore the intersection of AI and privacy concerns, we adopted a modified data collection approach inspired by Jarrodi et al. (2019), who utilized in-depth interviews to gather data from 17 nascent social entrepreneurs at a social innovation boot camp in France. This study employed a purposive sampling method, which inspired our data collection procedure. We carefully selected 42 expert interviewees from 979 respondents who offered valuable perspectives on AI and

information privacy issues. These individuals provided timely and comprehensive insights into the future implications of AI on data privacy. In contrast, Jarrodi et al.'s (2019) study was on political ideologies as a motivation for social entrepreneurship, while our study centered on AI and privacy concerns. This deliberate choice of sampling technique aligned with the characteristics of our target population and served the objectives of our investigation (Stake, 2010).

Unlike Zhu et al. (2021), who conducted a qualitative analysis of gender bias in medicine using a sample size of 23 participants, and Jarrodi et al. (2019), who investigated political ideologies in social entrepreneurship with a sample size of 17, our study employed a sample of 42 AI experts to examine the impact of AI adoption on information privacy. This sample size is sufficient for qualitative research and ensures the depth and richness of data necessary for meaningful insights while maintaining methodological rigor.

Determining the appropriate sample size in qualitative research is crucial to ensuring that findings are credible, reliable, and representative of the population under study. The decision to use 42 expert interviewees in this study is justified based on several methodological considerations, including data saturation, purposive sampling, comparability with existing research, and analytical rigor. One of the most widely accepted criteria for determining sample adequacy in qualitative research is data saturation: the point at which additional interviews yield no new insights, themes, or patterns (Guest et al., 2006). Studies have demonstrated that thematic saturation can often be achieved with 12–20 interviews, particularly in homogeneous populations. However, when dealing with experts from diverse industries, disciplines, or backgrounds, many interviewees are necessary to capture diverse perspectives (Mason, 2010). Hennink et al. (2017) suggested that a larger number of interviews, 30 to 50, is often necessary when aiming for maximum variation in expert studies. This range supports our claim that 42 interviews ensure thematic saturation related to our research topic.

In expert-based research, the quality of participants matters as much as the quantity. Purposeful sampling ensures that the study includes knowledgeable and experienced participants who can provide rich and insightful data (Patton, 2015). Since experts will provide in-depth, nuanced insights, studies often require a larger sample size than general qualitative studies to account for variations in expertise, roles, industries, and regional perspectives (Creswell & Poth, 2023). A sample of 42 experts ensures that the study captures diverse perspectives while maintaining analytical depth.

Furthermore, reviewing previous studies in the relevant field is a way to contextualize and justify the sample size. Research in business, policy analysis, and technology adoption frequently uses 20–50 expert interviews to ensure robust findings. For instance, Malterud et al. (2015) argued that information power, which considers the specificity and relevance of information obtained, suggests that expert interviews often require higher sample sizes to capture complex, multi-dimensional insights. Another key consideration is the balance between depth and breadth. A study with too few interviews may lack sufficient variation and depth, while an excessive number may overwhelm the analytical process (Braun & Clarke, 2019). The choice of 42 experts ensures a manageable dataset for thematic or qualitative content analysis while maintaining richness and diversity in responses. The decision to use 42 expert interviewees is justified based on data saturation, purposeful sampling, comparability with previous studies, and analytical manageability. Given the complexity of expert knowledge, this sample size ensures a comprehensive, credible, and well-rounded analysis while aligning with established qualitative research standards.

Using secondary data in research presents minimal ethical concerns as long as it is collected, stored, and analyzed following ethical guidelines (Andersen et al., 2011). Since secondary data is preexisting and is publicly available or obtained from reputable sources, issues related to informed consent, confidentiality, and participant harm are significantly reduced (Jol & Stommel, 2016). Researchers must ensure that information is accurately cited, properly anonymized if necessary, and used within its intended ethical framework. This study avoids data misuse or privacy violations by following established ethical considerations. Consequently, the data analysis remains ethically sound and valuable as best practices have been followed.

The AI experts were asked questions on AI and the future of humans. For example, they were asked to think forward: 'By 2030, do you think it is most likely that advancing AI and related technology systems will enhance human capacities and empower them? 'They were also asked to respond to this question: Is it most likely that advancing AI and related technology systems will lessen human autonomy, privacy, and agency to such an extent that most people will not be better off than the way things are today? (Anderson & Rainie, 2019, p. 4).

In the context of this study, the following characteristics of the sampled expert profiles were collected: gender of participants, age, nationality and country of residence, role/profession, and industry in which respondents operate. We focused on respondents who discussed issues on AI and privacy concerns. We initially identified that 54 respondents discussed AI and privacy issues. However, 12 of the respondents were anonymous and did not provide demographic information. We removed these 12 anonymous respondents and were left with 42 usable responses for analysis. We did not attempt to generalize our findings on AI and privacy concerns, but instead proposed a framework to explain the future advances of AI on information privacy.

To minimize bias and improve the reliability and validity of the qualitative data collected, the section below explains how the validity of the data collected was achieved to establish the credibility and trustworthiness of the findings.

Reliability and Validity

Unlike quantitative research, which, by employing statistical measures such as Cronbach's alpha, assesses test-retest reliability and internal consistency (Nunnally & Bernstein, 1994; Taber, 2018), qualitative research addresses reliability through different strategies due to the subjective nature of respondent opinions, which are inherently not replicable. This study prioritised the validity of thematic analysis by ensuring that identified themes directly address the research question. Furthermore, data validity was established by analyzing the frequency of specific themes across multiple expert responses.

We enhanced the reliability and validity of the qualitative data collected by utilizing member checking and multiple analysts (Barbour, 2001; Birt et al., 2016). Member checking involved engaging the research team in verifying findings to enhance validity. The authors ensured that the analyses accurately reflected participants' views by allowing team members to review and provide feedback on coding, analysis and interpretations of the results. Second, the multiple analyst approach, a form of intercoder reliability, was adopted to improve consistency in data interpretation. Members of the research team independently analyzed the same data, ensuring a robust and reliable analysis.

While we acknowledge that qualitative data is susceptible to bias and subjectivity (Zhu et al., 2021), we implemented measures to ensure the data's relevance. Initially, the primary researcher coded the data into developing themes that were then reviewed by the remaining three researchers to mitigate potential biases and to ensure stability and validity (Birt et al., 2016). Finally, the relevance of the thematic analysis of expert viewpoints was assessed by ensuring that the identified themes directly aligned with the research questions.

Furthermore, to minimize biases from the qualitative sources used in the research, we interpreted the coded data separately to achieve converging interpretations. Our reviews of the data collected were another essential strategy to mitigate any potential biases from the qualitative data. As noted by Mouselli and Massoud (2018), there are numerous biases in qualitative research; however, maintaining rigorous processes through which data are collected, analyzed, and presented reduces these biases. This approach has been adhered to and forms the epistemological basis of our research.

Step-by-Step Guide to the Development of Themes for Analysis

We adopted an open coding approach (Corbin & Strauss, 2015) and a two-stage inductive qualitative approach (Gioia et al., 2013) to code the responses. We began with open coding, analyzing interview transcripts line by line to identify and categorize emerging concepts and ideas related to AI and privacy concerns. Simultaneously, we

compared these initial codes with existing literature on AI and privacy to establish empirical and theoretical connections. This iterative process involved the following:

1. Familiarization: We repeatedly reviewed the interview transcripts to identify patterns and themes.
2. Note-taking: After familiarization with the data, we embarked on the recording of potential themes, common expressions, and language used by AI experts regarding AI and privacy concerns.
3. Initial coding: We generated initial code based on the identified patterns.

These initial codes were then refined and reorganized through iterative discussions among the research team, ultimately resulting in the identification of six core themes: human agency, data use and abuse, AI transparency and opacity, weaponization of information, cyberbullying and privacy concerns, and enforcement of privacy strategies. Thematic data analysis was conducted to explore and refine these themes.

Data Analysis

We adopted a thematic analysis approach in the analysis of the coded responses. Thematic analysis is a set of procedures in phases or stages for describing content based on themes (Oliveira et al., 2015; Valle & Ferreira, 2025). Thematic analysis was employed to analyze the data collected for this study, aligning well with qualitative research methods focused on identifying and interpreting themes and recurring patterns of meaning within the data. Themes are not merely repetitions of words or phrases but represent interpretive concepts that capture significant insights from the dataset (Braun & Clarke, 2006, 2019; Nowell et al., 2017). This approach was particularly suitable for our study as we aimed to explore subjective experiences, social processes, and the impact of AI on individuals and society.

Thematic analysis involves several steps, beginning with immersion in the data. This process includes reading and rereading transcripts or notes to develop a deep understanding of their content (Braun & Clarke, 2019). One of the key strengths of thematic analysis lies in its flexibility. Unlike some quantitative methods, it is not bound to a specific theoretical framework, which allows it to be adapted to diverse research paradigms. This flexibility makes it particularly effective for exploring complex or subjective topics such as AI adoption and its impact on information privacy, where a rich and detailed examination of the data is essential.

Additionally, thematic analysis is accessible to researchers at all levels of expertise. It does not require extensive technical training or specialised software, making it the best choice for novice researchers while remaining powerful enough for seasoned investigators (Braun & Clarke, 2006, 2019; Nowell et al., 2017). Its structured yet adaptable approach enables researchers to systematically identify, analyze, and interpret meaningful patterns within the data. The thematic analysis adopted proved invaluable due to its versatility and depth. It facilitated the systematic identification and interpretation of key patterns in the data, enabling us to explore the impact of AI on human experiences and social phenomena. This method's ability to balance structure with flexibility made it an essential tool for uncovering the complexities inherent in our research focus.

We analysed the 42 AI expert interview transcripts using a two-step thematic approach, drawing on principles from Eisenhardt's (1989) case study methodology. The first step focused on data immersion and initial coding for each interview separately. This began with coding for demographic attributes (gender, age, nationality, country of residence, role, and industry) to contextualise the dataset. Following this, each transcript was analyzed individually to identify initial themes, consistent with a 'within-case' logic. The second step involved a 'cross-case' synthesis, where themes from the initial phase were systematically compared across all interviews to refine them and develop broader, overarching findings.

The last stage is the treatment and interpretation of the coded responses. To ensure the reliability of the coded responses, each researcher repeated the coding process. Secondly, there was cross-coding by the other researchers, and finally, we checked the accuracy by comparing each coded response to each

other and removing any repetitions. To ensure the reliability of the coding we carried out the following processes: a) stability, which involves the same person repeating the coding process; b) reproducibility, which entails a different researcher repeating the coding process; and c) accuracy, which is when the result is compared to a standard (Krippendorff, 1980).

FINDINGS

This study aimed to investigate the impact of AI on information privacy within society. Our findings are outlined in two stages. We initially collected descriptive statistics to illustrate the demographic characteristics of the experts' responses regarding AI and information privacy. The results reveal that 73.8% of respondents were male and 26.2% were female (see Table 2). Hence, it can be inferred that males predominated in the AI industry. Furthermore, the findings indicate that the highest level of education among respondents was a doctorate (60%), whereas the lowest qualification was an undergraduate degree (12.3%).

Table 2. Descriptive statistics of respondents

Variables	Frequency	%	Variables	Frequency	%
Gender			**Nationality**		
Male	31	73.8	United States	23	54.6
Female	11	26.2	British	2	4.8
Total	**42**	**100**	Dutch	2	4.8
Educational level			French	2	4.8
Doctorate	25	60	Australian	1	2.4
Masters	12	28.5	Canadian	1	2.4
Undergraduate	1	2.3	Kenyan	1	2.4
Missing	4	9.2	Polish	1	2.4
Total	**42**	**100**	Portuguese	1	2.4
Industry			Russian	1	2.4
Education	20	47.6	Spanish	1	2.4
Information technology	13	31	Swedish	1	2.4
Business	1	2.4	Swiss	1	2.4
Charity	1	2.4	Venezuelan	1	2.4
Military	1	2.4	Missing	3	7
Public sector	1	2.4	**Total**	**42**	**100**
Research	1	2.4			
Venture capital	1	2.4			
Missing	3	7			
Total	**42**	**100**			

The second stage of the analysis adopted thematic content analysis. This analysis provided a broad range of information on the future of AI on information privacy, but sometimes

overlapping issues on AI's impact on privacy. Through thematic content analysis, we identified six emerging themes on the future of AI on information privacy: human agency, data use and abuse, AI transparency and opacity; weaponization of information, cyberbullying and privacy concerns, and enforcement of privacy strategies. The experts' comments were read and reread to identify the six themes by following Braun and Clarke's (2019) six-stage thematic analysis explained in the method section.

Human Agency

The analysis revealed human agency as one of the critical themes about AI's future. Experts articulated a dual perspective: on one hand, they remarked on AI's capacity to influence the future of work and improve communication. On the other hand, this potential was overshadowed by a pessimistic outlook on its implications for personal privacy, with many highlighting the fear that AI could soon operate beyond meaningful human control. As one of the experts remarked,

> *'I also see the potential for a much worse outcome in which the productivity gains produced by technology accrue almost entirely to a few, widening the gap between the rich and poor while failing to address the social ills related to privacy. I foresee a world in which IT and so-called AI produce an ever-increasing set of minor benefits, while simultaneously eroding human agency and privacy and supporting authoritarian forms of governance' (Anderson & Rainie, 2019, p. 36).*

A respondent who works at a major global privacy initiative predicted AI and tech will not improve most people's lives, citing loss of jobs, algorithms run amok, and subversion of privacy.

While all the experts strove to explain their views on the future benefits of AI in society, their understanding and anxiety about the impact of AI on privacy were also expressed. We mapped these concerns, identified them, and classified them as human agency, meaning the impact of AI on information privacy is human-centered. This finding is consistent with the work of Berkel et al. (2022), who investigated the implications of contextual morality for AI applications. They concluded that with the emergence of human-centered AI, the importance of a perspective based on fairness, accountability, context, and transparency will be crucial for contextualizing the morality of AI use in society.

Data Use and Abuse

Another theme developed in this study is the use and abuse of personal data. The analysis revealed that with advances in AI, there will be abuse of personal information by powerful agents, governments, businesses, and people in authority; however, there were no clear strategies to mitigate these concerns. Furthermore, there were variations in how experts articulated their views on the abuse and use of data because of advances in AI technology. For example, as one expert put it, 'Tracking and monitoring people will be an accepted part of life, and there will be stronger regulations on privacy and data security' (Anderson & Rainie, 2019, p.72). Another expert remarked, 'I am increasingly concerned that AI-driven decision making will perpetuate existing societal biases and injustices while obscuring these harms under the false belief that such systems are "neutral'' (Anderson & Rainie, 2019, p.28).

One of the major issues of data use and abuse is the use of personal data for surveillance and profiling. Governments and corporations increasingly collect and analyze large quantities of personal information to monitor individuals' behavior, preferences, and affiliations. While these practices can serve purposes such as targeted marketing or national security, they also erode privacy and risk enabling discriminatory practices. Individuals may be unfairly categorized or excluded based on algorithmic profiling, perpetuating biases and deepening societal inequalities (Zuboff, 2023). The overreach of surveillance further poses ethical dilemmas about autonomy and freedom in a digital society.

The psychological toll of data misuse is another area of growing concern. Continuous monitoring of online activities fosters a climate of surveillance anxiety in which individuals feel constantly watched and evaluated (Li et al., 2022). This sense of scrutiny can lead to self-censorship. People limit their expressions or behavior to avoid judgment or reprisal, thus curbing creativity and authenticity in

digital interactions. Over time, these pressures can erode mental well-being, manifesting as stress, fear, or feelings of helplessness (Stoycheff, 2016).

This finding highlights the growing integration of AI into business operations and daily life, raising significant concerns regarding potential risks, such as data misuse and privacy invasion. To uphold ethical and responsible research practices, it is essential to prioritize the careful identification, assessment, and management of these risks.

AI Transparency and Opacity

Experts' degree of openness or apathy to the impact of AI advances on information privacy was rendered more visible when they raised issues of transparency and opacity because of AI adoption. The respondents' views varied greatly about their perceptions of the future of AI on information transparency and opacity.

One of the experts described his anxiety about the future of AI and information transparency, stating, 'That is why the greatest challenge in the future for AI accountability is AI transparency. The challenge we face with the rise of AI is the growing opacity of processes and decision making' (Anderson & Rainie, 2019, p. 57). Another participant lamented,

> *'I also see the potential for a much worse outcome in which the productivity gains produced by technology accrue almost entirely to a few, widening the gap between the rich and poor while failing to address the social ills related to privacy. I foresee a world in which IT and so-called AI produce an ever-increasing set of minor benefits, while simultaneously eroding human agency and privacy and supporting authoritarian forms of governance'(Anderson & Rainie, 2019, p. 36).*

Weaponization of Information

Another interesting theme is the weaponization of information. This term refers to a process by which advances in AI will give individuals, organizations, and governments huge amounts of personal data that can be used as a weapon against users (Munro, 2005). This sentiment about how information will be used as a weapon was echoed by another expert:

> *Facets, including weaponized information, cyberbullying, privacy issues, and other potential abuses that will come out of this technology, will need to be addressed by global leaders. These uses of AI are rife with ethical and human rights issues, from perpetuating racial bias to violating our right to privacy and free expression.*

Cyberbullying and Privacy Issues

According to Goffman (2017) and Brown and Levinson (1987), cyberbullying is a type of act or situation that can happen accidentally or maliciously with the sole purpose of destroying or insulting one's reputation. Given the nature of the advances in AI and its impact on privacy, it is unsurprising that many of the experts expressed a strong negative affinity for the future of AI in terms of cyberbullying and privacy concerns. As one expert put it bluntly, 'With increasing cyberattacks and privacy concerns, AI could connect people to bad actors, which could cause stress and new problems.'

Enforcement of Privacy Strategies

Unsurprisingly, another theme that emerged from the data analysis is the enforcement of privacy strategies. This theme came up as a measure to address cyberbullying, weaponization of information, and the misuse and abuse of personal data. One expert commented,

> *AI systems promote innovation and growth, help address global challenges, and boost jobs and skills development. At the same time, establishing appropriate safeguards to ensure these systems are transparent and explainable, and respect human rights, democracy, culture, non-discrimination, privacy and control, safety, and security.*

The main issues here are that with the unlimited potential of AI technologies and associated privacy concerns, strategies such as holding users' data can lead to information breaches and difficulty in the

enforcement of privacy across borders (Organization for Economic Co-operation and Development, 2013). Further excerpts of the responses from the interviewees and the developing themes have been summarized in Table 3.

Table 3. Emerging Themes from Participants' Responses

Themes	Summary of responses
Data use and abuse	Individual use of AI will be to dominate/control people, and this will not make our lives better. Privacy is indeed dead, but in the place of personal privacy management, there will be network public governance ['public' is the opposite of privacy]. Tracking and monitoring of people will be an accepted part of life, and there will be stronger regulations on privacy and data security.
Weaponization of information	Facets, including weaponized information, cyberbullying, privacy issues, and other potential abuses that will come out of this technology, will need to be addressed by global leaders. These uses of AI are rife with ethical and human rights issues, from perpetuating racial bias to violating our right to privacy and free expression. 'It will also generate a great data industry (big data) market, and a lack of anonymity and privacy. These factors will create new social, cultural, security and political problems.' The shift of AI research to the private sector means that AI will be developed to further consumption, rather than extend knowledge and public benefit.
Enforcement of privacy strategies	But we also need to ensure that the future environment strongly protects privacy and security. 'The shift of AI research to the private sector means that AI will be developed to further consumption, rather than extend knowledge and public benefit.'
AI transparency and opacity	It's also important to have an honest dialogue between the experts, the media, and the public about the use of our data for social-good projects like health care, taking in the risks of acting, such as effects on privacy. 'That is why the greatest challenge ahead for AI accountability is AI transparency. The challenge we face with the rise of AI is the growing opacity of processes and decision-making.'
Cyberbullying and privacy issues	Cybersecurity needs to be at the forefront to prevent unscrupulous individuals from using AI to perpetrate harm or evil on humanity. 'With increasing cyberattacks and privacy concerns, AI could connect people to bad actors, which could cause stress and new problems.'
Human agency	A respondent who works at a major global privacy initiative predicted AI and tech will not improve most people's lives, citing 'loss of jobs, algorithms run amok.' AI will improve communication opportunities and sharing capabilities. AI systems will promote innovation and growth, help address global challenges, and boost jobs and skills development, while at the same time establishing appropriate safeguards to ensure these systems are transparent and explainable, and respect human rights, democracy, culture, nondiscrimination, privacy and control, safety, and security.

Note: AI = artificial intelligence
Source: (Anderson & Rainie, 2019)

The emerging themes in Table 3 illustrate that the responsible use of data holds the potential to drive progress and innovation. However, the risks associated with data misuse cannot be overlooked. Balancing data utilization with ethical considerations, robust regulations, and public accountability is critical for fostering a fair and secure digital society. An effective analysis of data usage and potential misuse is essential for stakeholders to ensure that data serves as a force for good (Marr, 2022). Similarly, Hepenstal et al. (2021) highlighted that the weaponization of information poses a growing risk, impacting individual trust and national security. Addressing this issue requires a multipronged approach including technological innovation, regulatory frameworks, public education, and international collaboration.

Privacy strategies demand a comprehensive approach that includes legal, technological, and cultural measures. Although challenges persist, technological advancement and enhanced global

cooperation will offer opportunities for a more secure, privacy-focused future. Effective privacy enforcement protects individual data, fosters trust, and ensures organizational integrity. Another critical theme to explore is cyberbullying and privacy issues, which present significant challenges in the digital age. Tackling these issues requires collaborative efforts involving individuals, governments, and corporations. Raising awareness, implementing effective policies, and leveraging technological solutions will lead to a safer and more respectful online environment (Marr, 2020).

The Institute of Electrical and Electronics Engineers (2019) further asserted that balancing AI transparency with opacity is pivotal for fostering trust, fairness, and accountability. Transparency helps to build trust and ensure regulatory compliance, while addressing opacity is essential for ethical AI development. Future efforts should prioritize innovations in explainable AI, establish robust ethical frameworks, and implement regulatory oversight to ensure AI systems are both trustworthy and beneficial.

The human agency theme emphasizes the complex interplay of factors influencing individual behavior, societal dynamics, and opportunities for change. While individuals can act independently, their choices are often shaped or constrained by structural, cultural, and situational factors. Enhancing human agencies through education, social support, and the creation of equitable systems can empower individuals and contribute to societal progress.

In conclusion, addressing the risks and opportunities identified in these emerging themes requires collective and sustained efforts across legal, technological, and societal domains. This approach can ensure that advances in AI and data use align with ethical principles, protect individual and societal interests, and contribute positively to a rapidly evolving digital landscape.

Privacy Elements

Utilizing CPM theory (Petronio, 1991, 2004, 2010) and the six identified themes – human agency, use and abuse of privacy, AI transparency and opacity, weaponization of information, cyberbullying and privacy issues, and enforcement of privacy strategies – we have identified four key building blocks of privacy, which we term Privacy Elements (see Table 4). These Privacy Elements are interconnected and mutually influential in individual decision-making. Specifically, perceived benefits enhance an individual's intention to disclose information and minimise perceived risks, affecting data management practices. For instance, individuals may weigh the advantages of information sharing against perceived risks when making disclosure decisions. Atalay and Yücel (2024) stated that location sharing with a navigation application exemplifies this balance of benefit versus privacy exposure. Moreover, when perceived benefits outweigh risks, individuals are more inclined to disclose personal information. Thus, higher perceived benefits correlate with a greater intention to disclose, and vice versa. On the other hand, a strong sense of data ownership tends to increase caution, potentially limiting disclosure intentions even in the presence of perceived benefits. This process underscores the complex interplay between perceived benefits, perceived risks, intention to disclose, and individual ownership perceptions in privacy-related decisions.

Table 4. Privacy Elements

Privacy elements	Description
Privacy benefits	Privacy benefits are regarded as a clear advantage for individuals and businesses, contributing to enhancing brand recognition, safeguarding against data breaches, fraud, and financial losses, and promoting trust.
Perceived privacy risks	Perceived privacy risk refers to the potential misuse of disclosed information or the anticipated loss of personal data upon disclosure.
Intention to disclose	The act of voluntarily consenting to share personal and/or private information.
Ownership of privacy	The circumstance by which a person perceives information to belong to themselves.

DISCUSSION

This study examined the multifaceted challenges and emerging themes surrounding information privacy in the context of advancing AI technologies. Through a thematic analysis, we identified key areas of concern, including human agency, the use and abuse of privacy, AI transparency and opacity, information weaponization, cyberbullying, and enforcement of privacy strategies.

A central finding underscores the influence AI will exert on future human activities. The impact of AI on society, specifically regarding increased data involvement and job displacement by robots, is a prevalent concern. Kaya Bicer et al. (2023) highlighted that AI's ability to gather, analyze, and combine vast quantities of data to support information-gathering capabilities in medicine raises ethical, patient privacy, and data safety concerns. Conversely, the significant capital investment required to implement and maintain AI systems with this capability presents a valid argument for retaining human involvement in data gathering and processing. Concerns surrounding this transition, particularly the potential for diminished human engagement and the implications for information privacy, have been widely echoed in literature across fields like human resources management (Berkel et al., 2022; Chelliah, 2017).

Furthermore, Harfouche et al. (2023) examined human-centric AI and bias reduction. They indicated that when AIs are trained on biased data, they can perpetuate and amplify privacy violations that disproportionately affect certain demographic groups. For instance, biased facial recognition might misidentify or unfairly surveil specific populations. A human-centric AI approach that actively works to alleviate bias is inherently linked to information privacy by ensuring fairer and more equitable treatment of individuals' data and reducing the risk of discriminatory privacy infringements. On the other hand, Sargent et al. (2024) investigated users' concerns about IoT privacy. They showed that privacy concerns, security concerns, awareness, and device use are all facets of how individuals perceive and react to the privacy risks inherent in interconnected devices. Understanding these concerns is fundamental to developing effective privacy safeguards, policies, and user education strategies in the rapidly expanding IoT landscape.

Also, the use and abuse of privacy, particularly concerning data ownership and usage, emerges as a significant theme. The increasing reliance on AI to collect confidential user data through operating systems such as Android and iOS generates privacy concerns due to unauthorised data collection and analysis. The Cambridge Analytica scandal, in which Facebook profiles were gathered without user consent, exemplifies this issue. Silva et al. (2015) proposed mechanisms to empower users to manage their sensitive information to mitigate potential abuses. Rosenzweig (2010) advocated updating data privacy laws to adapt to technological changes and to address data misuse. The growing dependence on AI amplifies data collection and analysis, introducing critical risks to individual privacy and societal well-being. Misuse of personal data can lead to identity theft, financial fraud, reputational harm, and psychological distress (Westin, 1968). Data breaches enabling malicious actors to exploit sensitive information often result in severe financial losses and emotional distress for victims (Solove & Schwartz, 2024). These breaches undermine public trust in organizations responsible for data protection.

Additionally, AI transparency and opacity represent critical challenges affecting information privacy in the context of advanced AI technologies. Increasing automation in decision making reduces human control and judgment (Amoore, 2019). This shift can lead to AI systems operating independently, raising issues with transparency and opacity (Burrell, 2016). We argue that AI's evolution will further diminish human oversight in information collection and privacy matters, exacerbating transparency challenges. Felzmann et al. (2019) highlighted the lack of clarity regarding the benefits of AI adoption, reinforcing transparency and opacity concerns across healthcare, traffic management, and retail. Also, Zhou et al. (2020) identified AI transparency as a crucial principle throughout the algorithm lifecycle, indicating its persistent relevance in business and individual communities.

Information weaponization is information control for a malicious purpose and is a significant concern. While AI adoption and privacy concerns have been extensively researched (Bélanger & Crossler, 2011), the weaponization of information in this context remains under-explored. Munro (2005) defined information weaponization as the control of information to blackmail, confuse, demoralize, and subvert. The interplay between AI adoption and privacy concerns creates a fertile ground for information weaponization, including disinformation and subversion (Cybenko et al., 2002; Munro, 2005). The inclusion of computer-mediated technology with human cognition facilitates automated decision making and data-driven learning, inevitably increasing the potential for information weaponization by institutions and individuals.

Cyberbullying and privacy concerns represent another significant challenge in the age of AI. The immeasurable nature of AI and digital spaces, coupled with the ability to control vast amounts of information, creates an environment conducive to cyberbullying (Forssell, 2018). Diminished user control over personal information facilitates the misuse of data for bullying and retaliatory purposes. Baron et al. (1999), Brown and Levinson (1987), and Kernaghan and Elwood (2013) emphasized the need for robust data protection legislation to prevent such abuses. Goffman (2017) and Ademiluyi et al. (2022) highlighted the potential for reputational damage through cyberbullying, which can alter social interactions, particularly in customer-client relationships.

Addressing privacy challenges in the age of AI requires robust enforcement strategies. Expert recommendations emphasize stakeholder collaboration and respect for individual privacy. Government institutions should develop stringent legislation to penalise data abusers (Bailey, 2012). Bailey advocated for a bill mandating disclosure of individual communications to state agents and broadening judicial powers to issue production and retention orders in privacy breach cases. However, these measures raise concerns about government-sponsored information weaponization.

The Organization for Economic Co-operation and Development (2013) proposed strategies including education, global interoperability of privacy management programs, and security breach notifications. Henttonen (2017) investigated privacy violations through contextual information transfer, suggesting privacy self-management, the right to be forgotten, data destruction, anonymization, and information havens to mitigate the risks of violations. In addition, Rosenzweig (2010) advocated for the revision of data privacy laws to address technological changes and data misuse.

Recent research on the importance of global information management in the context of AI and privacy also highlights the need for ownership of privacy due to the legal ramifications of the pervasiveness of AI in information management. Kerdvibulvech's (2024) research on big data and AI-driven analysis highlighted key geographical patterns in citation distribution, revealing the global recognition of AI-driven research in legal contexts. These findings imply that ownership of privacy across geographical locations is critical to professional and legal information management relating to AI and information privacy.

Furthermore, the European Union's General Data Protection Regulation (GDPR) establishes a comprehensive and stringent framework for privacy enforcement, characterised by broad scope, emphasis on individual rights, and centralised supervisory authorities with significant fining powers. This unified approach aims for consistent application across member states, fostering a strong culture of data protection. Academic discourse highlights GDPR's role in setting a global benchmark for privacy rights (Mantelero, 2017)

In contrast, the United States adopts a more sector-specific approach, with laws like the California Consumer Privacy Act focusing on consumer privacy in California and the federal Health Insurance Portability and Accountability Act addressing healthcare information. Enforcement is often decentralised, involving state attorneys general and federal agencies. This fragmented landscape can lead to inconsistencies and weaker overall protection than the GDPR's unified model (Schwartz, 2000). Also, Gupta and Pabigrahi (2023) explored global information management and sustainable business development. They indicated that effective global information management is crucial for adhering to diverse and often stringent international privacy regulations such as GDPR, the California

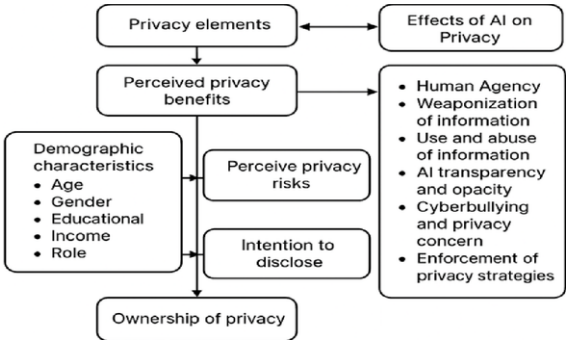
Consumer Privacy Act, and Brazil's General Personal Data Protection Law (LGPD). Sustainable business development necessitates building trust, and mishandling personal data can severely damage reputation and incur hefty fines, hindering sustainability. A well-designed decision support system should incorporate privacy-by-design principles to ensure that data protection is integral to business processes, thus linking information management to privacy.

Emerging economies are developing comprehensive data protection laws, often drawing inspiration from GDPR but also incorporating unique national contexts. Examples include Brazil's LGPD, India's Digital Personal Data Protection Act, and China's Personal Information Protection Law. Brazil's LGPD, influenced by GDPR, establishes broad privacy rights and enforcement mechanisms. India's Digital Personal Data Protection Act emphasises individual obligations alongside data fiduciary duties. China's Personal Information Protection Law implements stringent data processing rules and state control. Singh (2024) reflected on a global trend towards strengthening data protection, albeit with regional variations in enforcement priorities and effectiveness. Singh's comparative analysis revealed a spectrum of approaches, with GDPR representing a robust, unified model, the United States a more fragmented system, and emerging economies navigating their paths in the global data privacy landscape.

This analysis underscores the urgent need for comprehensive strategies to navigate the evolving landscape of privacy in the age of AI. Collaboration among stakeholders, robust legislation, and ethical data practices are essential to mitigate risk and ensure responsible AI adoption. Drawing from the six themes delineated in Table 3 – human agency, data use and abuse, AI transparency and opacity, weaponization of information, cyberbullying and privacy issues, and enforcement of privacy strategies – along with additional privacy elements outlined in Table 4, we propose a framework to guide future research on AI privacy concerns. This AI privacy model is structured around how users' demographic characteristics and key privacy elements (perceived privacy benefits, perceived privacy risks, intention to disclose, and ownership of privacy) influence advances in AI. These key elements have relationships with demographic characteristics and impact AI adoption. Categorizing AI and information users based on their demographic characteristics can enhance responsiveness to their privacy needs.

We build on CPM theory to develop the AI Information Privacy Framework (see Figure 1). This framework was designed through a multidisciplinary collaborative process integrating perspectives from fields including information sharing, data privacy, information management, and the broader information lifecycle. Rooted in established privacy models, the framework specifically addresses the unique risks AI technologies pose to personal data. It aims to provide a standardized and comprehensive set of guidelines that organizations and society can adopt to ensure the ethical use of AI. By focusing on respecting privacy rights while simultaneously fostering innovation, the framework seeks to balance the dual imperatives of technological advancement and the safeguarding of individual privacy. The privacy component is derived from existing CPM theory, aiding in the identification of crucial privacy concerns regarding AI adoption.

Figure 1. AI Information Privacy Framework



Note: AI = artificial intelligence

CONCLUSION

The purpose of this study is to examine how the adoption of AI will impact the future of information privacy. This study stands apart from earlier studies because it is one of the first to draw on CPM theory, arguing that advancing AI and related technology systems will lessen human autonomy and privacy to such an extent that the ownership of privacy will disappear in society. We offer a comprehensive theoretical framework for understanding the adoption of AI and its implications for information privacy. This study provides a holistic view of the complex interactions between AI adoption and privacy concerns. Our findings are consistent with the work of Gabisch and Milne (2014), who reported that when users are given some form of compensation in the form of a monetary reward, this compensation reduces their expectation of privacy concerns. The work of Petronio (2010) and Thompson et al. (2012) also provided another dimension to the problem of ownership of privacy. They suggested that privacy ownership is the ability to control conditions and to deny or allow access to private information. This ability enables a person to manage personal information even after giving access to others. We further forecast that future AI technology will take human control and judgment away from the process of information collection and that this development could reinforce the lack of transparency and information opacity in society.

Another contribution of this study is that with advances in AI technologies and the accessibility of computer-mediated technology to bad actors, the use of information as a weapon by institutions and individuals is inevitable in the future of AI's wider adoption. This development is evident in the work of Dresp (2023), who reported that technological progress aimed at benefiting mankind has produced what is now called the weaponization of AI.

Furthermore, this study contributes to the field of AI by formulating an AI privacy framework that incorporates demographic characteristics, human agency, the use and abuse of privacy, weaponization of information, AI transparency and opacity, and cyberbullying issues to explain how AI will impact information privacy. This framework will provide future researchers with a holistic view of the complex interactions between AI adoption and privacy concerns. We believe that our findings may act as an additional building block for theory building in future studies on AI and privacy. Specifically, we have provided in-depth insights into how AI adoption can influence privacy.

Policy Implications

Our findings carry significant implications for stakeholders, including adopters of AI technology, individuals, policymakers, social media platforms, organizations, and future researchers. For governments, organizations, and policymakers overseeing AI technologies, our findings underscore the broad privacy implications associated with the level of influence exerted by the utilization of AI. These

stakeholders must ensure that this transformative technology is not wielded as a weapon against society, as highlighted by Dresp (2023). Furthermore, our research indicates that as AI technology advances, privacy ownership may become obsolete, suggesting that users may be willing to trade their privacy for compensation.

Moreover, our study reveals concerns among AI experts regarding privacy enforcement strategies to protect users during the utilization of AI technologies. These concerns underscore the importance of implementing effective privacy enforcement measures, potentially through the enactment of appropriate laws mandating individuals' activities and communications to disclose information to agents of the state when the security of the state is at stake. Furthermore, access to such information should be restricted to dedicated government inspectors with the requisite background and credentials.

This research provides actionable insights for policymakers responsible for overseeing AI development and implementation to enact laws to guide individuals' privacy rights. By elucidating the prominent themes and concerns voiced by AI experts, this study informs policymaking endeavors geared towards fostering responsible AI implementation and safeguarding privacy in the digital era.

Theoretical Implications

This study holds theoretical significance for advancing future research in several ways. First, it suggests the potential for extending or refining CPM theory to address distinct privacy challenges arising from AI technologies. By incorporating insights from AI-specific privacy concerns, the CPM framework can be enhanced to offer more nuanced guidance for managing privacy in AI-driven contexts.

Second, there is a call to investigate the implications of AI adoption on individual agency, autonomy, and decision-making authority concerning personal information and privacy. Understanding how AI technologies influence individuals' control over their data and privacy can shed light on broader socio-technical dynamics and can inform the development of effective privacy protection measures in an increasingly AI-driven world.

Limitations and Future Research Directions

The current research has three main limitations that point to additional directions for future research in AI and privacy. First, given that most of the studies on AI and privacy were based on critical analysis of literature (Berkel et al., 2022) and were cross-sectional in design (Park et al., 2023; Paul & Ahmed, 2023), causal conclusions cannot be firmly drawn. We suggest that future research consider using panel data to examine trends regarding the future of AI and information privacy in different industries. Such data will help to contextualise and theorise future research on AI and privacy. To further deepen our understanding of the topic, future research should consider incorporating a quantitative research approach to gather numerical data and to investigate the direct impact of perceptions of AI adoption on information privacy.

Second, this study was based on secondary interview data, which did not allow generalization of the findings to other sectors and fields. We suggest that future studies should explore empirical quantitative investigations to enable the generalization of the findings. We also recommend that future research focus on examining the weaponization of information because of advances in AI technology.

Third, our findings suggest that the increased adoption of AI may lead to potential abuse and misuse of personal data. As AI technology advances and privacy concerns grow, users and researchers must carefully consider and manage the associated risks to ensure ethical and responsible research practices. We recommend that future research on AI adoption and information privacy examine ethical guidelines, data privacy, and security protocols for AI implementation.

COMPETING INTERESTS

The authors of this publication declare there are no competing interests.

FUNDING

This research was supported by Anglia Ruskin University through funding for the Open Access Article Processing Charge (APC).

PROCESS DATES

Received: August 8, 2024, Revision: April 23, 2025, Accepted: May 18, 2025

CORRESPONDING AUTHOR

Correspondence should be addressed to Alfred Akakpo; alfred.akakpo@northampton.ac.uk

REFERENCES

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behaviour in the age of information. *Science*, *347*(6221), 509–514. DOI: 10.1126/science.aaa1465 PMID: 25635091

Ademiluyi, A., Li, C., & Park, A. (2022). Implications and preventions of cyberbullying and social exclusion in social media: Systematic review. *JMIR Formative Research*, *6*(1), e30286. DOI: 10.2196/30286 PMID: 34982712

Agozie, D. Q., & Kaya, T. (2021). Discerning the effect of privacy information transparency on privacy fatigue in e-government. *Government Information Quarterly*, *38*(4), 101601. Advance online publication. DOI: 10.1016/j.giq.2021.101601

Amoore, L. (2019). Doubt and the algorithm: *On the partial accounts of machine learning. Theory, Culture & Society*, *36*(6), 147–169. DOI: 10.1177/0263276419851846

Anderson, J., & Rainie, L. (2019, Aug 5). *Artificial intelligence and the future of humans*. Pew Research Center. https://www.pewresearch.org/internet/2018/12/10/artificial-intelligence-and-the-future-of-humans/

Anderson, J., & Rainie, L. (2023, Feb 2). *As AI spreads, experts predict the best and worst changes in digital life by 2035*. Pew Research Center. https://www.pewresearch.org/internet/2023/06/21/as-ai-spreads-experts-predict-the-best-and-worst-changes-in-digital-life-by-2035/

Atalay, H. N., & Yücel, Ş. (2024). Decoding privacy concerns: The role of perceived risk and benefits in personal health data disclosure. *Archives of Public Health = Archives Belges de Santé Publique*, *82*(1), 180. DOI: 10.1186/s13690-024-01416-z PMID: 39394170

Attili, V. S. P., Mathew, S. K., & Sugumaran, V. (2022). Information privacy assimilation in IT organizations. *Information Systems Frontiers*, *24*(5), 1497–1513. DOI: 10.1007/s10796-021-10158-0

Bag, S., Routray, S., Srivastava, S. K., Roubaud, D., Benabdellah, A. C., & Grebinevych, O. (2025). Utilizing artificial intelligence for stakeholder engagement and social innovation in addressing climate change. *Journal of Global Information Management*, *32*(1), 1–31. DOI: 10.4018/JGIM.366588

Bailey, J. (2012). Systematic government access to private-sector data in Canada. *International Data Privacy Law*, *2*(4), 207–219. DOI: 10.1093/idpl/ips016

Barbour, R. S. (2001). Checklists for improving rigour in qualitative research: A case of the tail wagging the dog? *BMJ (Clinical Research Ed.)*, *322*(7294), 1115–1117. DOI: 10.1136/bmj.322.7294.1115 PMID: 11337448

Baron, R. A., Neuman, J. H., & Geddes, D. (1999). Social and personal determinants of workplace aggression: Evidence for the impact of perceived injustice and the type A behavior pattern. *Aggressive Behavior*, *25*(4), 281–296. DOI: 10.1002/(SICI)1098-2337(1999)25:4<281::AID-AB4>3.0.CO;2-J

Bélanger, F., & Crossler, R. (2011). Privacy in the digital age: A review of information privacy research in information systems. *Management Information Systems Quarterly*, *35*(4), 1017–1041. DOI: 10.2307/41409971

Berkel, N. V., Tag, B., Goncalves, J., & Hosio, S. (2022). Human-centred artificial intelligence: A contextual morality perspective. *Behaviour & Information Technology*, *41*(3), 502–518. DOI: 10.1080/0144929X.2020.1818828

Birt, L., Scott, S., Cavers, D., Campbell, C., & Walter, F. M. (2016). Member checking: A tool to enhance trustworthiness or merely a nod to validation? *Qualitative Health Research*, *26*(13), 1802–1811. DOI: 10.1177/1049732316654870 PMID: 27340178

Brandimarte, L., Acquisti, A., & Loewenstein, G. (2013). Misplaced confidences: Privacy and the control paradox. *Social Psychological & Personality Science*, *4*(3), 340–347. DOI: 10.1177/1948550612455931

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101. DOI: 10.1191/1478088706qp063oa

Braun, V., & Clarke, V. (2019). Reflecting on reflexive thematic analysis. *Qualitative Research in Sport, Exercise and Health*, *11*(4), 589–597. DOI: 10.1080/2159676X.2019.1628806

Brown, P., & Levinson, S. C. (1987). *Politeness: Some Universals in Language Usage* (*Vol. 4*). Cambridge University Press., DOI: 10.1017/CBO9780511813085

Burrell, J. (2016). How the machine thinks: Understanding opacity in machine learning algorithms. *Big Data & Society*, *3*(1), 1–12. DOI: 10.1177/2053951715622512

Cai, Y., Zhang, X., Niu, H., Li, W., Huo, D., He, J., & Chen, H. (2023). Privacy and information disclosure: Dynamic digital governance in response to COVID-19. *Journal of Global Information Management*, *31*(6), 1–22. DOI: 10.4018/JGIM.321182

Chelliah, J. (2017). Will artificial intelligence usurp white collar jobs? *Human Resource Management International Digest*, *25*(3), 1–3. DOI: 10.1108/HRMID-11-2016-0152

Chen, C., & Zheng, Y. (2023). When consumers need more interpretability of artificial intelligence (AI) recommendations? The effect of decision-making domains. *Behaviour & Information Technology*, *43*(14), 3481–3489. DOI: 10.1080/0144929X.2023.2279658

Collins, C., Dennehy, D., Conboy, K., & Mikalef, P. (2021). Artificial intelligence in information systems research: A systematic literature review and research agenda. *International Journal of Information Management*, *60*, 102383. DOI: 10.1016/j.ijinfomgt.2021.102383

Corbin, J., & Strauss, A. (2015). *Basics of qualitative research: Techniques and procedures for developing grounded theory*. Sage Publications.

Creswell, J. W., & Poth, C. N. (2023). *Qualitative inquiry and research design: Choosing among five approaches* (5th ed.). Sage Publications.

Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science*, *10*(1), 104–115. DOI: 10.1287/orsc.10.1.104

Cybenko, G., Giani, A., & Thompson, P. (2002). Cognitive hacking: A battle for the mind. *Computer*, *35*(8), 50–56. DOI: 10.1109/MC.2002.1023788

Degirmenci, K. (2020). Mobile users' information privacy concerns and the role of app permission requests. *International Journal of Information Management*, *50*, 261–272. DOI: 10.1016/j.ijinfomgt.2019.05.010

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, *17*(1), 61–80. DOI: 10.1287/isre.1060.0080

Dresp, B. (2023). The weaponization of artificial intelligence: What the public needs to be aware of. *Frontiers in Artificial Intelligence*, *6*, 1154184. DOI: 10.3389/frai.2023.1154184 PMID: 36967833

Eisenhardt, K. M. (1989). Building theory from case study research. *Academy of Management Review*, *14*(4), 532–550. DOI: 10.2307/258557

Felzmann, H., Villaronga, E. F., Lutz, C., & Tamò-Larrieux, A. (2019). Transparency you can trust: Transparency requirements for artificial intelligence between legal norms and contextual concerns. *Big Data & Society*, *6*(1), 1–14. DOI: 10.1177/2053951719860542

Fiechuk, A. (2019). The use of AI assistants in the courtroom and overcoming privacy concerns. *Widener Law Journal, 28*(1), 135–168. https://heinonline.org/HOL/LandingPage?handle=hein.journals/wjpl28&div=10&id=&page=

Fogli, D., & Tetteroo, D. (2022). End-user development for democratising artificial intelligence. *Behaviour & Information Technology*, *41*(9), 1809–1810. DOI: 10.1080/0144929X.2022.2100974

Forssell, R. C. (2018). Cyberbullying in a boundary blurred working life: Distortion of the private and professional face on social media. *Qualitative Research in Organizations and Management*, *15*(2), 1–19. DOI: 10.1108/QROM-05-2018-1636

Gabisch, A. J., & Milne, R. G. (2014). The impact of compensation on information ownership and privacy control. *Journal of Consumer Marketing*, *31*(1), 13–26. DOI: 10.1108/JCM-10-2013-0737

Gioia, D. A., Corley, K., & Hamilton, A. L. (2013). Seeking qualitative rigor in inductive research: Notes on the Gioia methodology. *Organizational Research Methods*, *16*(1), 15–31. DOI: 10.1177/1094428112452151

Goffman, E. (2017). *Interaction ritual: Essays in face-to-face behavior*. Routledge. eBook ISBN9780203788387

Guest, G., Bunce, A., & Johnson, L. (2006). How many interviews are enough? *Field Methods*, *18*(1), 59–82. DOI: 10.1177/1525822X05279903

Gupta, B. B., & Panigrahi, P. K. (2023). Analysis of the role of global information management in advanced decision support systems (DSS) for sustainable development. *Journal of Global Information Management*, *31*(2), 1–13. DOI: 10.4018/JGIM.320185

Harfouche, A., Quinio, B., & Bugiotti, F. (2023). Human-centric AI to mitigate AI biases: The advent of augmented intelligence. *Journal of Global Information Management*, *31*(5), 1–23. DOI: 10.4018/JGIM.331755

Hasan, Z., Vaz, D., Athota, V. S., Désiré, S. S. M., & Pereira, V. (2023). Can artificial intelligence (AI) manage behavioural biases among financial planners? *Journal of Global Information Management*, *31*(2), 1–18. DOI: 10.4018/JGIM.321728

Hennink, M. M., Kaiser, B. N., & Marconi, V. C. (2017). Code saturation versus meaning saturation. *Qualitative Health Research*, *27*(4), 591–608. DOI: 10.1177/1049732316665344 PMID: 27670770

Henttonen, P. (2017). Privacy as an archival problem and a solution. *Archival Science*, *17*(3), 285–303. DOI: 10.1007/s10502-017-9277-0

Hepenstal, S., Zhang, L., & William Wong, B. L. (2021). An analysis of expertise in intelligence analysis to support the design of Human-Centered Artificial Intelligence. *2021 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, Melbourne, Australia, pp. 107–112. https://doi.org/DOI: 10.1109/SMC52423.2021.9659095

Institute of Electrical and Electronics Engineers. (2019, Jun 11). *IEEE unveils third annual 'Generation AI' global study, illuminating trust millennial parents have in artificial intelligence for the health and wellness of their Generation Alpha kids*. https://www.prnewswire.com/news-releases/ieee-unveils-third-annual-generation-ai-global-study-illuminating-trust-millennial-parents-have-in-artificial-intelligence-for-the-health-and-wellness-of-their-generation-alpha-kids-300945886.html

Jang, C. (2023). Coping with vulnerability: The effect of trust in AI and privacy-protective behaviour on the use of AI-based services. *Behaviour & Information Technology*, *43*(11), 2388–2400. DOI: 10.1080/0144929X.2023.2246590

Jarrodi, H., Byrne, J., & Bureau, S. (2019). A political ideology lens on social entrepreneurship motivations. *Entrepreneurship and Regional Development*, *31*(7–8), 583–604. DOI: 10.1080/08985626.2019.1596353

Johnson, D., & Verdicchio, M. (2017). AI anxiety. *Journal of the Association for Information Science and Technology*, *68*(9), 2267–2270. DOI: 10.1002/asi.23867

Andersen, J. P., Prause, J., & Silver, R. C. (2011). A step-by-step guide to using secondary data for psychological research. *Social and Personality Psychology Compass*, *5*(1), 56-75. DOI: 10.1111/j.1751-9004.2010.00329.x

Jol, G., & Stommel, W. (2016). Ethical considerations of secondary data use: What about informed consent? *Dutch Journal of Applied Linguistics*, *5*(2), 180–195. DOI: 10.1075/dujal.5.2.06jol

Kaya Bicer, E., Fangerau, H., & Sur, H. (2023). Artificial intelligence use in orthopedics: An ethical point of view. *EFORT Open Reviews*, *8*(8), 592–596. DOI: 10.1530/EOR-23-0083 PMID: 37526254

Kerdvibulvech, C. (2024). Big data and AI-driven evidence analysis: A global perspective on citation trends, accessibility, and future research in legal applications. *Journal of Big Data*, *11*(1), 180. DOI: 10.1186/s40537-024-01046-w

Kernaghan, D., & Elwood, J. (2013). All the (cyber) world's a stage: Framing cyberbullying as a performance. *Cyberpsychology (Brno)*, *7*(1), 5. DOI: 10.5817/CP2013-1-5

Krippendorff, K. (1980). *Content analysis: An introduction to its methodology*. Sage Publications.

Ku, E. S. C., & Chen, C. D. (2024). Artificial intelligence innovation of tourism businesses: From satisfied tourists to continued service usage intention. *International Journal of Information Management*, *76*, 102757. DOI: 10.1016/j.ijinfomgt.2024.102757

LaBelle, S., White, A., & Forman, E. R. (2024). Graduate students' privacy boundaries in communicating about mental health with their advisors. *Communication Education*, *73*(2), 143–167. DOI: 10.1080/03634523.2023.2281325

Li, C., Chu, J., & Zheng, L. J. (2022). Better not let me know: Consumer response to reported misuse of personal data in privacy regulation. *Journal of Global Information Management*, *30*(1), 1–22. DOI: 10.4018/JGIM.309377

Lodder, A. R., & Wisman, T. H. A. (2015). Artificial intelligence techniques and the smart grid: Towards smart meter convenience while maintaining privacy. *Journal of Internet Law*, *19*(6), 20–27. https://ssrn.com/abstract =2714840

Madakam, S., Ramaswamy, R., & Tripathi, S. (2015). Internet of Things (IoT): A literature review. *Journal of Computer and Communications*, *3*(5), 164–173. DOI: 10.4236/jcc.2015.35021

Maldonado-Canca, L., Cabrera-Sanchez, J., Casado-Molina, A., & Bermúdez-González, G. (2024). AI in companies' production processes: What do their CEOs think? *Journal of Global Information Management*, *32*(1), 1–29. DOI: 10.4018/JGIM.366653

Malterud, K., Siersma, V. D., & Guassora, A. D. (2015). Sample size in qualitative interview studies: Guided by information power. *Qualitative Health Research*, *26*(13), 1753–1760. DOI: 10.1177/1049732315617444 PMID: 26613970

Mantelero, A. (2017). Regulating big data: The guidelines of the Council of Europe in the context of the European data protection framework. *Computer Law & Security Review*, *33*(5), 584–602. DOI: 10.1016/j.clsr.2017.05.011

Maragno, G., Tangi, L., Gastaldi, L., & Benedetti, M. (2023). Exploring the factors, affordances and constraints outlining the implementation of Artificial Intelligence in public sector organizations. *International Journal of Information Management*, *73*, 102686. DOI: 10.1016/j.ijinfomgt.2023.102686

Marr, B. (2020). *Tech Trends in Practice: The 25 technologies that are driving the 4th Industrial Revolution*. John Wiley & Sons.

Mason, M. (2010). Sample size and saturation in PhD studies using qualitative interviews. *Forum Qualitative Sozialforschung/Forum: Qualitative*. *Social Research*, *11*(3). DOI: 10.17169/fqs-11.3.1428

Mouselli, S., & Massoud, H. (2018). Common biases in business research. In Marx Gómez, J., & Mouselli, S. (Eds.), *Modernizing the Academic Teaching and Research Environment: Methodologies and Cases in Business Research* (pp. 97–109). Springer., DOI: 10.1007/978-3-319-74173-4_6

Müller, V. C. (2016). Editorial: Risks of artificial intelligence. In Muller, V. C. (Ed.), *Risks of Artificial Intelligence* (1st ed.). Chapman and Hall/CRC., DOI: 10.1201/b19187-4

Munro, I. (2005). *Information warfare in business: Strategies of resistance and control in the network society*. Routledge. DOI: 10.4324/9780203449233_chapter_1

Nowell, L., Norris, J. M., White, D. E., & Moules, N. J. (2017). Thematic analysis: Striving to meet the trustworthiness criteria. *International Journal of Qualitative Methods*, *16*(1), 1609406917733847. Advance online publication. DOI: 10.1177/1609406917733847

Nunnally, J. C., & Bernstein, I. H. (1994). *Psychometric theory* (3rd ed.). McGraw-Hill.

Oliveira, M., Bitencourt, C., Santos, A. C., & Teixeira, E. K. (2015). Thematic content analysis: Is there a difference between the support provided by the MAXQDA® and NVivo® software packages*? Revista de Administração da UFSM*, *9*(1), 72–82. DOI: 10.5902/1983465911213

Organization for Economic Co-operation and Development. (2013). *Privacy expert group report on the review of the 1980 OECD privacy guidelines*. OECD Digital Economy Papers, No. 229, OECD Publishing. DOI: 10.1787/20716826

Park, G., Yim, M. C., Chung, J., & Lee, S. (2023). Effect of AI chatbot empathy and identity disclosure on willingness to donate: The mediation of humanness and social presence. *Behaviour & Information Technology*, *42*(12), 1998–2010. DOI: 10.1080/0144929X.2022.2105746

Patton, M. Q. (2015). *Qualitative research and evaluation methods*. Sage Publications.

Paul, A., & Ahmed, S. (2023). Computed compatibility: Examining user perceptions of AI and matchmaking algorithms. *Behaviour & Information Technology*, *43*(5), 1002–1015. DOI: 10.1080/0144929X.2023.2196579

Petronio, S. (1991). Communication boundary management: A theoretical model of managing disclosure of private information between married couples. *Communication Theory*, *1*(4), 311–335. DOI: 10.1111/j.1468-2885.1991.tb00023.x

Petronio, S. (2004). Road to developing communication privacy management theory: Narrative in progress, please stand by. *Journal of Family Communication*, *4*(3–4), 193–207. DOI: 10.1207/s15327698jfc0403&4_6

Petronio, S. (2010). Communication privacy management theory: What do we know about family privacy regulation? *Journal of Family Theory & Review*, *2*(3), 175–196. DOI: 10.1111/j.1756-2589.2010.00052.x

Rahman, M. J., Rana, T., Xu, Y., & Ohman, P. (2024). Bridging BI and AI enhancing operational efficiency in the Chinese financial sector. *Journal of Global Information Management*, *32*(1), 1–27. DOI: 10.4018/JGIM.366871

Rosenzweig, P. (2010). Privacy and counter-terrorism: The pervasiveness of data. *Case Western Reserve Journal of International Law*, *42*(3), 625. https://scholarlycommons.law.case.edu/jil/vol42/iss3/6

Sargent, C. S., Koohang, A., & Svanadze, S. (2024). Users' concerns and the Internet of Things (IoT) risk beliefs. *Journal of Global Information Management*, *32*(1), 1–19. DOI: 10.4018/JGIM.359210

Schwartz, P. M. (2000). Internet privacy and the state. *Connecticut Law Review*, *32*(3), 815–860. https://heinonline.org/HOL/LandingPage?handle=hein.journals/conlr32&div=34&id=&page=

Silva, P., Amorim, V. J. P., Ribeiro, F. N., & Muzetti, I. (2015). *PrivacyMod: Controlling and monitoring abuse of privacy-related data by Android applications. 2015 Brazilian Symposium on Computing Systems Engineering (SBESC)*, Foz do Iguaçu, 42–47. DOI: 10.1109/SBESC.2015.15

Singh, B. (2024). Cherish data privacy and human rights in the digital age: Harmonizing innovation and individual autonomy. In Pucelj, M., & Bohinc, R. (Eds.), *Balancing Human Rights, Social Responsibility, and Digital Ethics* (pp. 199–226). IGI Global Scientific Publishing., DOI: 10.4018/979-8-3693-3334-1.ch007

Smilansky, O. (2017, Mar 13). *The real benefits of artificial intelligence.* CRM Information Today. https://www.destinationcrm.com/Articles/Editorial/Magazine-Features/The-Real-Benefits-of-Artificial-Intelligence-121403.aspx

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *Management Information Systems Quarterly*, *20*(2), 167–196. DOI: 10.2307/249477

Smith, S. A., & Brunner, S. R. (2017). To reveal or conceal: Using communication privacy management theory to understand disclosures in the workplace. *Management Communication Quarterly*, *31*(3), 429–446. DOI: 10.1177/0893318917692896

Solove, D. J. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review*, *154*(3), 477–560. DOI: 10.2307/40041279

Solove, D. J., & Schwartz, P. M. (2024). *Information privacy law* (8th ed.). Aspen Publishing.

Soumelidou, A., & Tsohou, A. (2024). Towards an information privacy competency model for the usage of mobile applications. In N. Meyer & A. Grocholewska-Czuryło (Eds.), *ICT Systems Security and Privacy Protection* (222-235). SEC 2023. IFIP Advances in Information and Communication Technology, vol. 679. Springer, Cham. https://doi-org.northampton.idm.oclc.org/10.1007/978-3-031-56326-3_16

Stake, R. (2010). *Qualitative research: Studying how things work*. The Guilford Press.

Steeves, V. (2019). Theorizing privacy in a liberal democracy: Canadian jurisprudence, anti-terrorism, and social memory after 9/11. *Theoretical Inquiries in Law*, *20*(1), 323–341. DOI: 10.1515/til-2019-0011

Stoycheff, E. (2016). Under surveillance: Examining Facebook's spiral of silence effects in the wake of NSA internet monitoring. *Journalism & Mass Communication Quarterly*, *93*(2), 296–311. DOI: 10.1177/1077699016630255

Sun, S., Drake, J. R., & Hall, D. (2022). When job candidates experience social media privacy violations: A cross-culture study. *Journal of Global Information Management*, *30*(1), 1–25. DOI: 10.4018/JGIM.312251

Taber, K. S. (2018). The use of Cronbach's alpha when developing and reporting research instruments in science education. *Research in Science Education*, *48*(6), 1273–1296. DOI: 10.1007/s11165-016-9602-2

Thompson, J., Petronio, S., & Braithwaite, D. O. (2012). An examination of privacy rules for athletic/academic advisors and college student-athletes: A communication privacy management perspective. *Communication Studies*, *63*(1), 54–76. DOI: 10.1080/10510974.2011.616569

Tsai, J. Y., Serge, E., Lorrie, C., & Alessandro, A. (2011). The effect of online privacy information on purchasing behavior. *Information Systems Research*, *22*(2), 254–268. DOI: 10.1287/isre.1090.0260

Valle, P. R. D., & Ferreira, J. D. L. (2025). Content analysis in the perspective of Bardin: Contributions and limitations for qualitative research in education. *Educação em Revista*, *41*, e49377. DOI: 10.1590/0102-469849377

Walrave, M., Verswijvel, K., Ouvrein, G., Staes, L., Hallam, L., & Hardies, K. (2022). The limits of sharenting: Exploring parents' and adolescents' sharenting boundaries through the lens of communication privacy management theory. *Frontiers in Education*, *7*, 803393. Advance online publication. DOI: 10.3389/feduc.2022.803393

Wang, B., Rau, P. P., & Yuan, T. (2023). Measuring user competence in using artificial intelligence: Validity and reliability of artificial intelligence literacy scale. *Behaviour & Information Technology*, *42*(9), 1324–1337. DOI: 10.1080/0144929X.2022.2072768

Westin, A. F. (1968, Jun 10). Privacy And Freedom. *Washington and Lee Law Review*, *25*(1), 166. https://scholarlycommons.law.wlu.edu/wlulr/vol25/iss1/20

Wu, P. F., Vitak, J., & Zimmer, M. T. (2019). A contextual approach to information privacy research. *Journal of the Association for Information Science and Technology*, *71*(4), 485–490. DOI: 10.1002/asi.24232

Zhou, J., Chen, F., Berry, A., Reed, M., Zhang, S., & Savage, S. (2020). A survey on ethical principles of AI and implementations. In *Proceedings of the 2020 IEEE Symposium Series on Computational Intelligence (IEEE SSCI)*, Canberra, Australia, 1–4 December. DOI: 10.1109/SSCI47803.2020.9308437

Zhu, P., Wu, Q., Liu, X., Waidley, E., Ji, Q., & Xu, T. (2021). Gender bias and the lack of equity in pandemic nursing in China: A qualitative study. *International Journal of Environmental Research and Public Health*, *18*(19), 10273. DOI: 10.3390/ijerph181910273 PMID: 34639570

Zuboff, S. (2023). The age of surveillance capitalism. *In Social Theory re-wired* (pp. 203-213. Routledge. eBook ISBN9781003320609 DOI: 10.4324/9781003320609-27

Alfred is currently a Senior Lecturer in Business Analytics at University of Northampton. His research interests are in data mining, business intelligence and forecasting of emerging technologies.

Evans Akwasi Gyasi is an Associate Professor in International Trade at the School of Economics, Finance and Law. He is the Deputy Head of School in charge of UG International Business programs and the school's NSS. Prior to joining the University, he spent close to a decade at Coventry University, overseeing the MBA Senior Leader apprenticeship course and teaching on the International Business and Business Analytics courses at Coventry Business School. He received his PhD from the University of Warwick (AACSB, EQUIS and AMBA accredited). He is a Fellow of Chartered Management Institute (CMI) and Senior Fellow of the Higher Education Academy (SFHEA). Research interests Evans' research focuses on developing and emerging economies such as Africa, Asia and South America. He has undertaken collaborative research projects from the University of Warwick, Coventry University, University of Bradford, De Montfort University, University of Kent, University of Ghana, Kwame Nkrumah University of Science and Technology and Ciputra Universitas, and has been invited to deliver presentations in the UK, Ghana, Canada, Turkey and Indonesia. His research work has been published or forthcoming in leading scholarly journals such as European Management Review, Journal of International Technology and Information Management, Journal of Business Research, and Journal of International Management. Evans' research examines the nexus of big data, business models, operations and decision making within international businesses in developing and emerging markets. His interests lie in contributing towards theory and practice by informing business decisions, providing insights into the future, and solving industrial, societal problems using data.