

Consumer Privacy Risks and Privacy Protection in the Era of Artificial Intelligence

Xia LIU

*School of Economics and Management, University of Chinese Academy of Sciences,
Beijing 100190, China*

E-mail: liuxia18@mailsucas.ac.cn

Hong ZHAO

*Sino-Danish College, University of Chinese Academy of Sciences, Beijing 100190, China; School of
Economics and Management, University of Chinese Academy of Sciences, Beijing 100190, China*

E-mail: zhaohong@ucas.ac.cn

Abstract Artificial intelligence has transformed marketing and consumer lives. However, despite its multiple beneficial effects, unprecedented artificial intelligence uses pose enormous challenges to consumer privacy protection. This research aims to provide a comprehensive picture of privacy research and enhance privacy protection. We first give more specific definitions of consumer privacy according to data analytic processes. Second, we investigate how AI-related factors, privacy risk, privacy protection, and other factors influence consumer privacy decision-making, and draw a conceptual model based on the extended Antecedents-Privacy Concerns-Outcomes (APCO) model. Third, we examine the potential risks of each data analytic step and the causes of privacy risks from consumer, company, and technology perspectives, and propose privacy protection schemes correspondingly. Lastly, we also provide agenda for future research.

Keywords artificial intelligence; consumer privacy; consumer privacy risks; consumers privacy protection

1 Introduction

Artificial intelligence (AI) has been widely used by marketers worldwide. According to Salesforce's recent report, at least 70% of marketers have been using AI to automate consumer interactions and data integration, personalize the consumer journey across channels, or predict consumer behaviors^[1]. Most companies have seen significant revenue increases from AI adoption^[2]. However, since AI applications in marketing rely on data collection, data verification, data storage and control, deriving insights, and disseminating insights^[3], these processes risk consumer privacy. Numerous privacy issues have alarmed consumers, companies, and govern-

Received March 31, 2023, accepted December 13, 2023

Supported by the National Natural Science Foundation of China (71972175)

ments. For example, a hacker wanted to sell the data stolen from 5.4 million Twitter accounts in 2022^[4]. As a result of the current situation, 86% of participants report growing concern for their privacy, according to the Klynveld Peat Marwick Goerdeler survey^[5].

With the increasing privacy issues and growing privacy concern, governments and companies have endeavored to enhance privacy protection. Countries worldwide have legislated, or are legislating, data protection laws to regulate how companies collect, store, transfer, and use consumer data. For example, Europe has enforced the General Data Protection Regulation (GDPR) since 2018, which protects consumers by enforcing companies to comply with data minimization and anonymization principles. Technology companies also are taking more measures to protect privacy. Apple has launched a new Tracking Transparency framework which requires app-tracking authorization requests to the user and gives consumers more control over how their data is tracked and collected.

Our research is driven by the tension between privacy risks and protection, and the need to understand consumer privacy and what consumers would do regarding their privacy with the tension they are exposed with. Second, we also identify a few gaps in the literature. There is no systematic review of how AI-related factors, privacy risks and privacy protection factors affect consumer privacy decision-making. Each study explores their roles with one specific theoretical lens. The current literature also lacks systematic review of what privacy risks could happen during data analytic processes. As such, we explore the vast literature on consumer privacy to capture what we know and what needs to be extended.

We contribute to privacy literature by first consolidating the traditional privacy concepts with AI reality to provide more specific definitions of consumer privacy in the AI era. Second, we explore what we have already known from the empirical findings and reorganize the findings to understand effects of AI-related factors, privacy risk and privacy protection factors based on the extended APCO model. We enrich the original antecedents, mainly consumer-related factors, in the extended APCO model by including AI-related factors, privacy risk and privacy protection factors. By doing this, we provide an overview of how various factors work in consumer privacy decision-making behavior. Third, we also examine the potential privacy risks from each data analytic process and the cause of privacy risks in consumer, companies, and government aspects. Finally, we provide guidelines on privacy protection accordingly and future research agenda.

2 Consumer Privacy Research

For the following part, we will first elaborate on the definition of consumer privacy and then investigate how privacy risk, privacy protection, and other factors influence consumer privacy decision-making.

2.1 The Definition of Consumer Privacy

General privacy includes physical privacy and information privacy. Physical privacy concerns physical access to an individual or their personal space, while information privacy refers to access to personal information^[6]. We only focus on information privacy and will use the

term privacy to refer to information privacy for the rest of this study. Researchers have been studying the definition of privacy from various perspectives (e.g., law, psychology, marketing, and information systems), though there is no unified definition. Smith, et al.^[6] summarized and categorized the definitions of general privacy from four aspects: State, a right, a commodity, and control. Consumer privacy shares the complexity with general privacy as an extension or specification of general privacy. The unprecedented application of AI technologies poses more difficulties in defining consumer privacy and calls for a more refined definition. Phelps, Nowak, and Ferrell^[7] defined consumer privacy as “*the ability to affect the dissemination and use of personal information that is collected during, or as a result of, marketing transactions, as well as control over unwanted telephone, mail, or personal intrusions in the consumer’s home.*” This concept only focuses on the dissemination and use of consumer data. Quach, et al.^[8] further classify consumer privacy into *information privacy*: Consumers’ right to control the access to, use, and dissemination of their data; *individual privacy*: Right of a person to be left alone without disruption; and *communication privacy*: protections for communications against interception and eavesdropping.

In contrast to the former research, to provide more specific and clear definitions in the AI era, we define consumer privacy by consolidating the traditional privacy definition and data analytics processes (data collection, storage, verification, deriving insights, and disseminating insights^[3]). First, consumer privacy means that consumers are in a state of not being tracked or at least know how and what kinds of data are being collected if they choose to disclose their data for benefits, such as personalized service (in correspondence to data collection). Second, consumer privacy also means consumers have control^[9,10] over the dissemination of data, verification, and aggregation of their data, how their data is used to derive insight, and what insights can be derived (in correspondence to data storage, verification, deriving insights). Third, consumers have the right to be left alone without disruptions of unwanted marketing communications, such as unsolicited telephone calls, emails, or personalized advertising (in correspondence to disseminating insights).

2.2 How the Influencing Factors Affect Consumer Privacy Decision-making

The main consumer privacy decision is whether to disclose information (e.g., share information, fabricate information, protect information, and withdraw information), click ads or accept personalized recommendations, or adopt AI technologies. Scholars have been investigating various influencing factors of consumer privacy decision-making. For example, Martin and Murphy^[11] group the influencing factors into social factors (e.g., ethical frameworks, global variation, legal and policy implications), consumer psychology factors (e.g., privacy concerns, consumer vulnerability, individual differences, and organizational privacy communication), privacy-enhancing factors (e.g., organizational trust, personalization value, consumer control, and data transparency), and privacy failure (e.g., data breach, identity theft, and hyper-competitive actions). Smith, Dinev, and Xu^[6] identified individual traits and contextual factors, such as privacy experiences, personality, demographic differences, and culture. In contrast, we categorize

the influencing factors into AI-related factors, privacy protection factors, privacy risk factors, and other factors (Table 1). We adopt Dinev, McConnell, and Smith's^[12] extended APCO model which surpasses the original APCO and recognizes consumer irrationality by including variables from behavioral economics and psychology to organize four groups of the influencing factors. The resulting model is shown in Figure 1. Next, we will explain AI-related factors, privacy protection factors, privacy risk factors, and other factors and how they influence consumer privacy decision-making.

AI-related factors: AI applications in marketing have ushered in a transformative paradigm in consumer engagement, concurrently presenting a puzzle concerning the preservation of consumer privacy. The interplay between AI and consumer privacy is complicated. We hereby discuss the relationship from four aspects: AI application types, online vs offline AI applications, consumer-AI experience, and AI characteristics. First, AI applications in marketing could be consumer-facing (e.g., personalization, service robots) or non-consumer-facing (e.g., price prediction, store layout optimization)^[13]. Although both types of applications could benefit con-

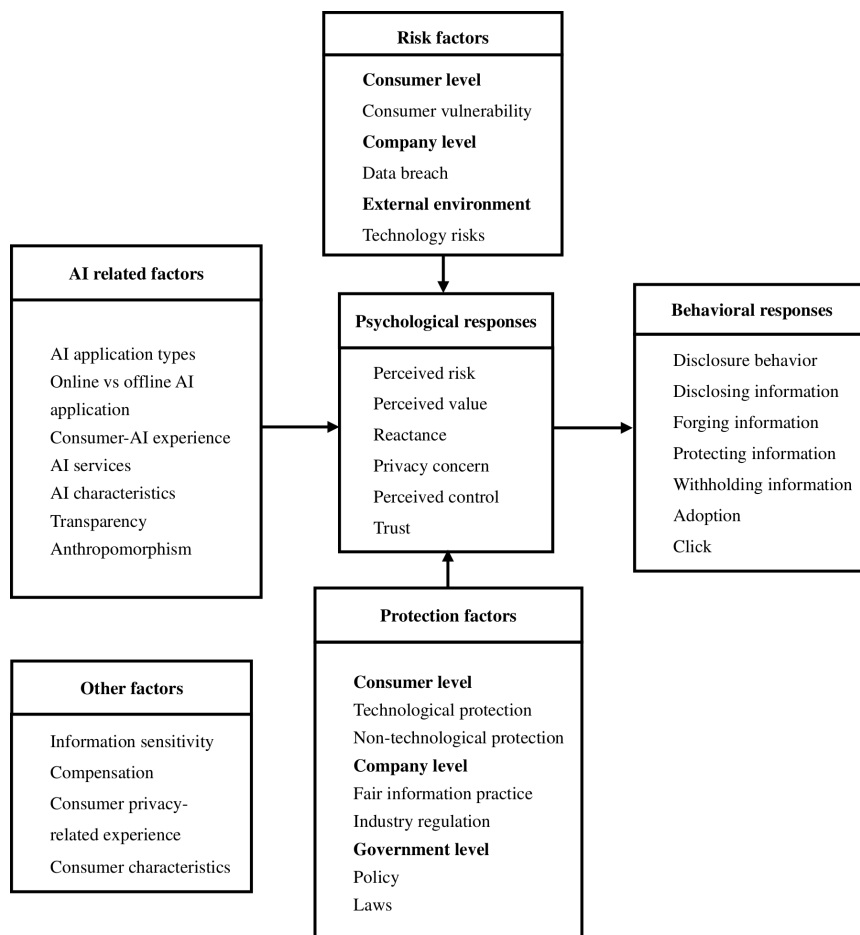


Figure 1 Conceptual model

Table 1 Privacy protection factors, privacy risk factors, and other factors

Factors		Papers
AI related factors		
	AI application types, Online vs Offline AI application, Consumer-AI experience: AI services (e.g., personalization, smart assistant), AI characteristics (e.g., anthropomorphism)	Guha, et al. ^[13] , Puntoni, et al. ^[14] , Xie, et al. ^[15]
Protection factors		
Consumer	Non-technological approach: Use privacy setting, browser setting (deleting cookies), read privacy policy. Technological approach: Check for spyware data capture, virus protection, install firewall	Crossler ^[16] , Xu, et al. ^[17] , Milne, Rohm, and Bahl ^[18]
Company	Fair information practice: Privacy assurance, privacy seal(industry self-regulation)	Adjerid, et al. ^[19] , Hui, Teo, Lee ^[20] , Aiken and Boush ^[21] , Lwin, Wirtz, and Williams ^[22] , Xu, et al. ^[17] , Culnan and Bies ^[23] , Xu, et al. ^[24]
Government	Policy and law	Wirtz, Lwin, Williams ^[25] , Lwin, Wirtz, and Williams ^[22] , Xu, et al. ^[17] , Xu, et al. ^[24]
Risk factors		
Consumers	Consumer vulnerability	Martin, Borah, Palmatier ^[26] , Martin and Murphy ^[11] , Sundar, et al. ^[27] , Adjerid, Peer, and Acquisti ^[28]
Companies	Collect data without permission, unauthorized secondary use (internal), data breach, consumer data aggregation	Gopal, et al. ^[29] , Smith, Milburg, and Burke ^[30]
Other parties	Unauthorized secondary use (external), identity theft	Milne, Rohm, and Bahl ^[18] , Smith, Milburg, and Burke ^[30]
Other factors		
	Transparency, Compensation, personalized services; Information types (sensitive vs. non-sensitive); Consumer characteristics, demographic difference, former experience; Time; Culture	Xu, et al. ^[24] , Kim, Barasz, and John ^[31] , Awad and Krishnan ^[32] , Vance, et al. ^[33] , Karwatzki ^[34] , Buckman, Bockstedt, and Hashim ^[35] , Markos, Milne, and Peltier ^[36] , Smith, Dinev, and Xu ^[6]

sumers, consumer-facing applications might induce more privacy concern than non-consumer-facing applications if there is any mistake. Second, offline AI applications may cause more

consumer privacy concern. For example, online personalization is more widely accepted, but if consumers get personalized recommendations based on their walking route, they might exhibit higher privacy concern. Third, as consumers consistently interact with AI, experiences with data analytic processes might influence consumer privacy differently. For example, consumers may feel vulnerable due to the massive data collection that is intrusive and unavoidable beyond their understanding^[14], leading to privacy concern. However, when consumers encounter personalized service, they evaluate perceived value and perceived risk and choose to adopt when the benefits outweigh perceived costs^[37]. Fourth, AI characteristics also influence consumers in different ways. For example, transparency of the AI system can empower consumers with more sense of control by informing them what data the company uses. With more privacy control, consumers will likely to share their information or engage more in marketing activities^[31]. However, the effectiveness of transparency is limited. Transparency benefits companies when they reveal acceptable information, but it backfires when they reveal unacceptable information^[31]. Anthropomorphism is also a double-edged sword by, on the one hand, increasing consumer's trust^[38] and decreasing the feeling of privacy invasion^[15], and, on the other hand, serving as a creating the feeling of reactance^[39].

Protection factors: According to Xu, et al.^[17], we further classify protection factors into consumer, company, and government aspects. Consumers protect their privacy through two main approaches: non-technological and technological approaches^[23]. The non-technological approaches include reading privacy policies, removing information from Web sites, refusing to do business with online firms, complaining indirectly to third-party organizations, etc., and technological approaches include various privacy-enhancing technologies (PETs), such as the firewall, virus protection, cookie management tools^[18,23,40]. Companies's privacy protection approaches that consumers could see or feel are privacy assurances (e.g., privacy policy consent, privacy statement, privacy seals). Governments could protect privacy by making new policies and regulations, legislation, and law enforcement.

The effects of the protection factors on consumer decision-making are mediated by perceived risks, perceived value, perceived control, privacy concern, and reactance. For example, Xu, et al.^[17] find that consumer protection approaches could empower consumers with direct control over their privacy, and perceived control, as a key factor affecting privacy concern over personal information, has negative effects on privacy concern. Tucker^[41] also found the change in Facebook's privacy policy to increase users' privacy control nearly doubles the clicks on personalized ads. Apart from that, Hui, Teo, and Lee^[20] found that privacy statements will decrease consumers' perceived risk of their information being misused and lead to higher information disclosure, whereas privacy seal does not affect information disclosure. And Goldfarb and Tucker^[42] find banner ads' effectiveness reduces because EU privacy law limits companies' ability to target the right consumers.

Risk factors: Risk factors include consumer vulnerability, unauthorized data collection, secondary use (both internal and external), combining consumer data, and data breach, and these

factors are dependent on each other. Consumer vulnerability implies that consumers' data is susceptible to harm or injury resulting from the intrusion or theft of their information saved on their personal computers, theft of their online transactions or cookie information, and companies breaking privacy policies^[18]. Martin, Borah, and Palmatier^[26] further classified consumer vulnerability into data manifest vulnerability, data breach vulnerability, spillover vulnerability, and data access vulnerability. Internal unauthorized secondary use refers to the data collected for one purpose being used for other purposes. In contrast, external unauthorized secondary use refers to the data collected by one company being shared with an external party^[30]. Combining consumer data refers to combining consumer data in separate databases into larger database to get new information about the consumer^[30]. Martin, Borah, and Palmatier^[26] found that vulnerabilities will damage consumer trust and increase falsifying behavior, negative WOM, and switching behavior. Chen, Beaudoin, and Hong^[43] found that the experience of being an internet scam victim will increase online privacy concern, and consumers will adopt more information protection behaviors. Mousavi, et al.^[44] classified privacy risk evaluation into threat susceptibility and severity, and find that privacy risk evaluation increases protection motivation and coping appraisal, thus negatively affects information disclosure. Consumer vulnerability could also refer to the lack of ability to make rational decisions due to biases, heuristics, misattribution, bounded rationality, and information asymmetries^[12,45]. Research has found that consumers who are exposed with fuzzy boundary heuristic are less likely to disclose personalization information than those with benefit heuristic^[27] and when consumers perceive higher levels of privacy protection than a reference point, they are more willing to disclose personal information^[28].

Other factors: Other factors include company compensation (both money or coupon), information type, demographic differences, and culture or climate differences. The benefits provided by companies could positively affect consumer information disclosure by increasing perceived value. Research has shown that money could increase information disclosure^[24,37], and monetary incentives are only effective for consumers between 12 to 21 years old and not for consumers between 22 to 54 years old^[46]. Furthermore, disclosure intention for different types of information varies. For example, consumers are more willing to disclose demographic and lifestyle information and less willing to disclose financial information, purchase information, and personal identifiable information. When marketers request more (vs. less) sensitive information, consumers have higher risk beliefs and less trusting beliefs, thus decrease information disclosure intention. Apart from that, consumer age^[47,48], education^[48] and internet experience^[48], and culture differences^[49] also influence consumer privacy-related decisions and also moderate the relationships between risk factors, protection factors, and AI factors, and psychological responses.

In conclusion, as the conceptual model shows, various factors influence consumer privacy decision-making and their effects are moderated by factors like culture and consumer demographics. However, consumer privacy decision-making is more complicated than what is presented

in the model. Privacy decision-making is not a one-time decision, but ongoing and evolving decisions that consumer will face in their lives. For example, a consumer could make a decision to protect privacy (as a behavioral response) due to the influencing factors at a certain time, the protection strategy could also work as an influencing factor for future decision-making. Moreover, the interplays between the influencing factors add more difficulties to present a one-time fit all model. For example, consumer experience with AI application which collect massive data can make them feel exploited and vulnerable. And privacy regulations could certainly influence AI applications and finally consumer decision-making. The proposed model shows the current state of consumer privacy research in the AI era, but by no means, could give a perfect explanation of privacy decision-making process.

3 Consumer Privacy Risks in the Era of Artificial Intelligence

3.1 Privacy Risks

Nowadays, consumers access to information and services from various platforms, reveling in the conveniences that technologies afford them. However, in doing so, they may consciously or unconsciously comprise their privacy. Disclosing information could benefit consumers because companies could offer better services if they knew more about consumers. However, sometimes companies collect, store, and use consumer data secretly and even sell consumer data. We discuss the potential risks along with the data analytic processes: 1) data collection, 2) data verification, 3) data storage and control, 4) deriving insights, and 5) disseminating insights (see Table 2).

Table 2 Potential privacy risks along data analytic processes

Author	Potential risks
Data collection	Consumer lack of control over companies' access to consumer information and data exchange in different devices and feel the vulnerability of potential cyberattacks.
Data verification	Risk of identity theft and misinformation of a consumer which are beyond consumer control.
Data storage and control	Data breaches, unauthorized access, and cybersecurity threats, long-term storage.
Deriving insights	AI has the ability to predict sensitive data based on non-sensitive information. Use enormous amounts of consumer data to train AI models with informing consumers.
Disseminating insights	Consumers get unsolicited communications and incorrect recommendations or untimely messages, potentially leading to the inadvertent exposure of their privacy to others.

In today's digital landscape, *data collection* from a multitude of platforms has become a pervasive and intricate process. Consumers navigate through an interconnected web of technology, where interactions and engagements with online services contribute to a vast repository of per-

sonal information. Consumers lack the control over companies' access to all sorts of data. For example, their demographic and online surfing information could be tracked without awareness when enjoying online shopping services. Their biometrics information could be illegally tracked when using mobile phones or facial detection techniques. And consumers' information posted on social media might be exploited by e-commerce and insurance companies^[50]. *Data verification* often requires the exchange and sharing of sensitive information, such as personal identifiers, contact details, and even biometric data which might cause identify theft. Moreover, both innate errors in collected data and operation errors in data verification process might lead to misinformation of a consumer^[3]. *Data storage and control*, especially when it involves personal, sensitive, or confidential information, creates a potential vulnerability. Data breaches, unauthorized access, and cybersecurity threats can compromise the privacy of consumers. And the long-term data storage could raise ethical concerns. *Deriving insights* heavily relies on AI technologies which has the ability to predict sensitive information based on insensitive information, such as pregnancy, tendency of getting divorced^[8,13]. And companies might use consumer data to train AI models with informing consumers. Further, companies could use the superior knowledge obtained from consumer data aggregation to perform personalized pricing, which might decrease consumer welfare. Lastly, *disseminating insights* could also compromise consumer privacy by interrupting consumers by unsolicited communications (e.g., emails, marketing calls, text messages, social media messages). Consumers might get incorrect recommendations or untimely messages, potentially leading to the inadvertent exposure of their privacy to others.

3.2 The Causes of Privacy Risks

We categorize the causes of privacy risks into consumer, company, and technology factors.

Consumers could endanger their privacy because of their vulnerabilities. First, since some consumers are overconfident in companies' privacy protection and less aware of privacy risks, they do not protect their privacy proactively^[51,52]. For example, they use the same simple password for many websites and do not use privacy settings. They also do not read privacy policies and assume their privacy is well-protected if they do not explicitly feel the invasion. Second, consumers have limited abilities to protect their privacy even if they intend to^[53]. They have difficulties comprehending complicated and lengthy privacy policies and using advanced personal privacy-enhanced technologies. Third, consumers tend to make decisions based on prior experience and are easily biased because lack of objectiveness. Dinev, McConnell, and Smith^[12] found that consumers are influenced by peripheral cues, heuristics, and misattribution, thus, make decisions with bounded rationality.

Companies threaten consumer privacy in several ways. First, some companies may collect, use, and share consumer data without authorization damaging consumer privacy^[30]. Second, since domestic data privacy laws in different countries vary substantially^[54], small application development companies could sign a contract with cloud storage providers from countries with less rigorous regulation and jeopardize consumer privacy^[55]. Third, a company's employees may endanger consumer privacy because of accidentally losing laptops or storage devices used

at work^[56]. Fourth, the lack of skilled IT labor and management expertise required by a newly adopted technology can also increase the chance of data breach^[56].

Loopholes in the network environment and network communication protocols, insufficient mobile access security, unsafe location services, and unsafe data storage and transmission could also endanger consumer privacy^[51,54,55,57]. For example, smart wearable devices and smart home devices equipped with many sensors and transmission technologies are tightly connected, which poses challenges to consumers because hackers can easily access all sorts of data^[58,59]. Apart from that, consumer data is often stored on cloud servers. Cloud storage lacking physical or space limitations is more easily invaded by hackers^[55].

4 Consumer Privacy Protection in Artificial Intelligence Era

Followed by the overview of privacy risk and its causes, we further put forward privacy protection strategies from consumer, company, and government perspectives.

4.1 Consumer Privacy Protection Strategies

First, consumers should educate themselves to increase privacy protection awareness. Privacy-related training could boost consumer privacy protection motivation and nudge them to adopt more protection strategies, such as fabricating or refusing to disclose information^[18,60]. Apart from that, consumers should develop a “healthier” surfing habit to protect their privacy by 1) reading privacy policy clauses; 2) staying away from illegal software and website; 3) using complicated passwords and do not use the same password for many websites; 4) refusing to give unnecessary permission (e.g., location, microphone, camera); 5) deleting cookies without delay; 6) complaining to companies or a third party^[51]. Second, consumers could apply AI technologies such as privacy-enhanced technology to control company access to their information and use ad blocker to avoid targeted advertisements and reduce the amount of data collected about their online behavior. For example, newly developed AI technologies such as “Solid” and “Datum” make consumers the owner of their data, rather than companies^[61]. Third, consumers should be aware of their biases when making decisions and avoid being influenced by situational factors. Last but not important, a consumer should ask the relevant government bureau to protect their rights if privacy invasion had happened.

4.2 Company Privacy Protection Strategies

A company could protect consumer privacy in various ways. First, a company could follow the standard procedure to collect, store and use consumer data ethically and legally. They could simplify privacy policy clauses and optimize privacy setting surface. Second, IT and security investment are crucial to avoid being attacked by hackers. Companies should also adapt their organization practices along with IT to optimize the IT protection effect. In addition, in the product design and development process, enterprise technicians should review the product repeatedly to prevent technical loopholes from leaking consumer privacy. More importantly, companies could use AI technologies to protect consumer privacy. For example, using

anonymization and pseudonymization to remove or encrypt personal identifiable information. Anonymization methods encompass recoding, swapping, randomizing data, k-anonymization, Markov chain monte Carlo, differential privacy, generative adversarial networks etc.^[3,62–65]. Companies could also use natural language processing for data scanning to detect sensitive information and mask them to protect privacy.

Industry self-regulation is a commonly applied approach mainly focusing on regulating privacy practices by industry codes of conduct and self-policing trade groups and associations^[17]. Industry self-regulation groups and associations could audit companies' privacy protection operations and provide technical support to enhance privacy protection.

4.3 Government Privacy Protection Strategies

The government protects consumer privacy mainly through legislation and law enforcement. Countries worldwide have, or are legislating, data protection laws to regulate how companies collect, store, transfer, and use consumer data. For example, Europe has enforced GDPR since 2018 and specifies that data is a personal asset. California Consumer Privacy Act, aiming to regulate how companies handle consumer data, is in force in 2020. The Personal Information Protection Law of the People's Republic of China takes effect in 2021. The government should continue to improve legislation along with technology breakthroughs. Besides that, governments should also enhance law enforcement to fight against the entire privacy criminal chain. Lastly, the government should be attentive to publicity of privacy protection laws to improve consumer privacy protection awareness and how to use the law to protect their legitimate rights and interests.

5 Future Research Agenda in Artificial Intelligence Era

The advent of the AI era has introduced new challenges for consumer privacy protection, as AI technologies rely heavily on data, often personal or sensitive, to function effectively. Consumer data is a valuable resource with the potential to significantly improve consumers' lives and drive economic growth and innovation. Conversely, AI technology introduces substantial privacy concerns due to its association with unauthorized data collection, the extensive datasets required for AI training and operation, the heightened risk of data breaches and cyberattacks, and the potential for biases in AI outcomes. Consequently, this has propelled consumer self-protection, companies to change their practices and privacy legislation. Consumers find themselves in a tension between consumer privacy protection and privacy risks. However, it is unclear what are the absolute effects of privacy protection and privacy risk factors on psychological privacy responses and which protection strategy is more effective in terms of reducing privacy concern? Thus, we call for quantitative research (e.g., meta-analysis) to answer the above questions. Moreover, the effect of regulations like GDPR on the companies' compliance still needs to be investigated.

Furthermore, different protection strategies might have different spillover effects which are worth investigating. First, the new technologies which empower consumers by making them the owners of their data have raised a hot debate over who should own the data. Some advocate

that consumer undoubtedly should own their data which could improve consumer welfare^[66]. However, recent privacy ownership shift find that it might not effectively enhance consumer welfare but potentially harm it and its impact depends on the service provider's revenue structure, discount in the service quality, and the way consumers get compensated^[61]. Second, whether the companies prioritizing consumer privacy could get competitive advantages by attracting privacy-conscious consumers still needs to be tested. And if they could benefit from implementing strong privacy protection strategies, will the benefits vary across different types of companies, such as, data-intensive companies and non-data-intensive companies? Third, recent research finds that GDPR's effect goes beyond reducing the number of third-party domains requested by websites and also changes the market structure, with big companies getting significantly more market share^[67]. This calls for research on the relationship between privacy protection and competition and how to design privacy laws.

6 Conclusion

We first examine consumer privacy literature and give a more specific definition of consumer privacy from data analytic process. Second, we explore how AI-related factors, privacy risk and privacy protection factors influence consumer privacy decision-making. We found these factors affect privacy-related behavior through perceived risk, perceived value, reactance, privacy concern, perceived control, and trust. Notably, consumer privacy decision-making is rather complicated and the influencing factors also affect each other. Third, we further explore the potential risks along five data analytic process and causes of privacy risks and provide correspondent protection strategies. Lastly, based on the insights of our paper, we also provide future research agenda. Overall, we hope this research could provide a picture of current privacy research and guidance on privacy protection, and shed light on future research in AI era

References

- [1] Salesforce, The 8th Edition State of Marketing Report, Available at: <https://www.insiderintelligence.com/chart/260290/AI-Uses-Marketers-Worldwide-Aug-2022-of-respondents>, 2022 [Accessed 2024-09-28].
- [2] McKinsey, Survey: AI adoption proves its worth, but few scale impact. Available at: <https://www.mckinsey.com/featured-insights/artificial-intelligence/global-ai-survey-ai-proves-its-worth-but-few-scale-impact>, 2019 [Accessed 2024-09-28].
- [3] Wieringa J, Kannan P K, Ma X, et al. Data analytics in a privacy-concerned world. *Journal of Business Research*, 2021, 122: 915–925.
- [4] Powell O. The biggest data breaches and leaks of 2022. Available at: <https://www.cshub.com/attacks/articles/the-biggest-data-breaches-and-leaks-of-2022>, 2022 [Accessed 2024-09-28].
- [5] KPMG, Data Privacy Survey. Available at: <https://info.kpmg.us/news-perspectives/industry-insights-research/data-privacy-survey-orson-lucas.html>, 2022 [Accessed 2023-01-11].
- [6] Smith H J, Dinev T, Xu H. Information privacy research: An interdisciplinary review. *MIS Quarterly*, 2011, 35(4): 989–1015.

- [7] Phelps J, Nowak G, Ferrell E. Privacy concerns and consumer willingness to provide personal information. *Journal of Public Policy & Marketing*, 2000, 19(1): 27–41.
- [8] Quach S, Thaichon P, Martin K D, et al. Digital technologies: Tensions in privacy and data. *Journal of the Academy of Marketing Science*, 2022, 50(6): 1299–1323.
- [9] Westin A F. Privacy and freedom. New York: Antheneum, 1967.
- [10] Irwin Altman. The environment and social behavior: Privacy, personal space, territory, and crowding. Monterey, Brooks/Cole Publishing, California, 1975.
- [11] Martin K D, Murphy P E. The role of data privacy in marketing. *Journal of the Academy of Marketing Science*, 2017, 45(2): 135–155.
- [12] Dinev T, McConnell A R, Smith H J. Research commentary — Informing privacy research through information systems, psychology, and behavioral economics: Thinking outside the “APCO” box. *Information Systems Research*, 2015, 26(4): 639–655.
- [13] Guha A, Grewal D, Kopalle P K, et al. How artificial intelligence will affect the future of retailing. *Journal of Retailing*, 2021, 97(1): 28–41.
- [14] Puntoni S, Reczek R W, Giesler M, et al. Consumers and artificial intelligence: An experiential perspective. *Journal of Marketing*, 2021, 85(1): 131–151.
- [15] Xie Y, Zhu K, Zhou P, et al. How does anthropomorphism improve human-AI interaction satisfaction: A dual-path model. *Computers in Human Behavior*, 2023, 148: 107878.
- [16] Crossler R E, Bélanger F. Why would I use location-protective settings on my smartphone? Motivating protective behaviors and the existence of the privacy knowledge-belief gap. *Information Systems Research*, 2019, 30(3): 995–1006.
- [17] Xu H, Teo H-H, Tan B C Y, et al. Effects of individual self-protection, industry self-regulation, and government regulation on privacy concerns: A study of location-based services. *Information Systems Research*, 2012, 23(4): 1342–1363.
- [18] Milne G R, Rohm A J, Bahl S. Consumers’ protection of online privacy and identity. *Journal of Consumer Affairs*, 2004, 38(2): 217–232.
- [19] Adjerdid I, Acquisti A, Telang R, et al. The impact of privacy regulation and technology incentives: The case of health information exchanges. *Management Science*, 2015, 62(4): 1042–1063.
- [20] Hui K-L, Teo H H, Lee S-Y T. The value of privacy assurance: An exploratory field experiment. *MIS Quarterly*, 2007, 31(1): 19–33.
- [21] Aiken K D, Boush D M. Trustmarks, objective-source ratings, and implied investments in advertising: Investigating online trust and the context-specific nature of Internet signals. *Journal of the Academy of Marketing Science*, 2006, 34(3): 308–323.
- [22] Lwin M, Wirtz J, Williams J D. Consumer online privacy concerns and responses: A power-responsibility equilibrium perspective. *Journal of the Academy of Marketing Science*, 2007, 35(4): 572–585.
- [23] Culnan M J, Bies R J. Consumer privacy: Balancing economic and justice considerations. *Journal of Social Issues*, 2003, 59(2): 323–342.
- [24] Xu H, Teo H-H, Tan B C Y, et al. The role of push-pull technology in privacy calculus: The case of location-based services. *Journal of Management Information Systems*, 2009, 26(3): 135–174.
- [25] Wirtz J, Lwin M O, Williams J D. Causes and consequences of consumer online privacy concern. *International Journal of Service Industry Management*, 2007, 18(4): 326–348.

- [26] Martin K D, Borah A, Palmatier R W. Data privacy: Effects on customer and firm performance. *Journal of Marketing*, 2017, 81(1): 36–58.
- [27] Sundar S S, Kang H, Wu M, et al. Unlocking the privacy paradox: Do cognitive heuristics hold the key?. *CHI'13 Extended Abstracts on Human Factors in Computing Systems*. New York, NY, USA: Association for Computing Machinery, 2013: 811–816.
- [28] Adjerid I, Peer E, Acquisti A. Beyond the privacy paradox: Objective versus relative risk in privacy decision making. *MIS Quarterly*, 2018, 42(2): 465–A5.
- [29] Gopal R D, Hidaji H, Patterson R A, et al. How much to share with third parties? User privacy concerns and website dilemmas. *MIS Quarterly*, 2018, 42(1): 143–A25.
- [30] Smith H J, Milburg S J, Burke S J. Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly*, 1996, 20(2): 167–196.
- [31] Kim T, Barasz K, John L K. Why am I seeing this ad? The effect of ad transparency on ad effectiveness. *Journal of Consumer Research*, 2019, 45(5): 906–932.
- [32] Awad, Krishnan. The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization. *MIS Quarterly*, 2006, 30(1): 13–28.
- [33] Vance A, Jenkins J L, Anderson B B, et al. Tuning out security warnings: A longitudinal examination of habituation through fMRI, eye tracking, and field experiments. *MIS Quarterly*, 2018, 42(2): 355–380.
- [34] Karwatzki S, Dytynko O, Trenz M, et al. Beyond the personalization-privacy paradox: Privacy valuation, transparency features, and service personalization. *Journal of Management Information Systems*, 2017, 34(2): 369–400.
- [35] Buckman J R, Bockstedt J C, Hashim M J. Relative privacy valuations under varying disclosure characteristics. *Information Systems Research*, 2019, 30(2): 375–388.
- [36] Markos E, Milne G R, Peltier J W. Information sensitivity and willingness to provide continua: A comparative privacy study of the United States and Brazil. *Journal of Public Policy & Marketing*, 2017, 36(1): 79–96.
- [37] Chellappa R K, Sin R G. Personalization versus privacy: An empirical examination of the online consumer's dilemma. *Information Technology and Management*, 2005, 6(2–3): 181–202.
- [38] Liu K, Tao D. The roles of trust, personalization, loss of privacy, and anthropomorphism in public acceptance of smart healthcare services. *Computers in Human Behavior*, 2022, 127: 107026.
- [39] Puzakova M, Rocereto J F, Kwak H. Ads are watching me A view from the interplay between anthropomorphism and customisation. *International Journal of Advertising*, 2013, 32(4): 513–538.
- [40] Son J-Y, Kim S S. Internet users' information privacy-protective responses: A taxonomy and a nomological model. *MIS Quarterly*, 2008, 32(3): 503–529.
- [41] Tucker C E. Social networks, personalized advertising, and privacy controls. *Journal of Marketing Research*, 2014, 51(5): 546–562.
- [42] Goldfarb A, Tucker C E. Privacy regulation and online advertising. *Management Science*, 2011, 57(1): 57–71.
- [43] Chen H, Beaudoin C E, Hong T. Securing online privacy: An empirical test on Internet scam victimization, online privacy concerns, and privacy protection behaviors. *Computers in Human Behavior*, 2017, 70: 291–302.

- [44] Mousavi R, Chen R, Kim D J, et al. Effectiveness of privacy assurance mechanisms in users' privacy protection on social networking sites from the perspective of protection motivation theory. *Decision Support Systems*, 2020, 135: 113323.
- [45] Kokolakis S. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, 2017, 64: 122–134.
- [46] Koh B, Raghunathan S, Nault B R. An empirical examination of voluntary profiling: Privacy and quid pro quo. *Decision Support Systems*, 2020, 132: 113285.
- [47] Goldfarb A, Tucker C. Shifts in privacy concerns. *American Economic Review*, 2012, 102(3): 349–353.
- [48] Malhotra N K, Kim S S, Agarwal J. Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research*, 2004, 15(4): 336–355.
- [49] Bleier A, Goldfarb A, Tucker C. Consumer privacy and the future of data-based innovation and marketing. *International Journal of Research in Marketing*, 2020, 37(3): 466–480.
- [50] Smith M, Szongott C, Henne B, et al. Big data privacy issues in public social media. 2012 6th IEEE International Conference on Digital Ecosystems and Technologies (DEST), 2012: 1–6.
- [51] Xiang M, Wang X, Jia R, et al. Research on the risk evaluation of consumers' privacy information disclosure in mobile commerce. *Library and Information Service*, 2018, 62(18): 34–44.
- [52] Ferrell O C. Broadening marketing's contribution to data privacy. *Journal of the Academy of Marketing Science*, 2017, 45(2): 160–163.
- [53] Martin K. Privacy notices as tabula rasa: An empirical investigation into how complying with a privacy notice is related to meeting privacy expectations online. *Journal of Public Policy & Marketing*, 2015, 34(2): 210–227.
- [54] Berry R, Reisman M. Policy challenges of cross-border cloud computing. *Journal of International Commerce & Economics*, 2012, 4: 1–38.
- [55] Banerjee S, Hemphill T, Longstreet P. Wearable devices and healthcare: Data sharing and privacy. *The Information Society*, 2018, 34(1): 49–57.
- [56] Kim S H, Kwon J. How do EHRs and a meaningful use initiative affect breaches of patient information? *Information Systems Research*, 2019, 30(4): 1184–1202.
- [57] Zhang T, Zhao K, Yang M, et al. Research on privacy security risk assessment method of mobile commerce based on information entropy and Markov. *Wireless Communications and Mobile Computing*, 2020, 2020: 1–11.
- [58] Ching K W, Singh M M. Wearable technology devices: Security and privacy vulnerability analysis. *International Journal of Network Security & Its Applications*, 2016, 8(3): 19–30.
- [59] Islam K, Shen W, Wang X. Security and privacy considerations for Wireless Sensor Networks in smart home environments. *Proceedings of the 2012 IEEE 16th International Conference on Computer Supported Cooperative Work in Design (CSCWD)*. 2012: 626–633.
- [60] Desimpelaere L, Hudders L, Van de Sompel D. Knowledge as a strategy for privacy protection: How a privacy literacy training affects children's online disclosure behavior. *Computers in Human Behavior*, 2020, 110: 106382.
- [61] Li S, Liu Y, Feng J. Who should own the data? The impact of data ownership shift from the service provider to consumers. *Journal of Management Information Systems*, 2023, 40(2): 366–400.
- [62] Ponte G, Wieringa J, Boot T, et al. Where's Waldo? A framework for quantifying the privacy-

- utility trade-off in marketing applications. *International Journal of Research in Marketing*, 2024, 41(3): 529–546.
- [63] Grewal R, Gupta S, Hamilton R. Marketing insights from multimedia data: Text, image, audio, and video. *Journal of Marketing Research*, 2021, 58(6): 1025–1033.
- [64] Schneider M J, Jagpal S, Gupta S, et al. A flexible method for protecting marketing data: An application to point-of-sale data. *Marketing Science*, 2018, 37(1): 153–171.
- [65] Anand P, Lee C. Using deep learning to overcome privacy and scalability issues in customer data transfer. *Marketing Science*, 2023, 42(1): 189–207.
- [66] Haberer B, Krämer J, Schnurr D. Standing on the shoulders of web giants: The economic effects of personal data brokers. *SSRN Electronic Journal*, 2020.
- [67] Peukert C, Bechtold S, Batikas M, et al. Regulatory spillovers and data governance: Evidence from the GDPR. *Marketing Science*, 2022, 41(4): 746–768.