scientific reports

OPEN

Public attitude and media governance of biometric information dissemination in the era of digital intelligence

Wenyi Zhang[1], Hengtian Zhang[2]✉ & Zhouyang Deng[3]

Absrtact: In the era of digital intelligence, biometrics plays a critical role in mediating sensitive information dissemination, human-computer interaction, and governance in both virtual and real-world settings, including the evolving metaverse. Based on an empirical analysis of 1,862 participants, the current study investigated factors influencing public perception, acceptance, and risk awareness of biometric technologies. The findings highlight the critical roles of perceived trust (PT) and technical prudence (TP) in driving behavioral intentions (BI), with their positive effects outweighing the significant deterrent impact of perceived risks (PR). While PT and perceived availability (PA) significantly enhance the adoption of biometric technologies, TP exhibited an unexpected positive influence, suggesting that cautious users may still embrace biometrics if perceived as secure and trustworthy. These results emphasize the urgency of refining legal and regulatory frameworks, improving risk mitigation strategies, and enhancing user confidence to foster the responsible adoption and utilization of biometric technologies. This study offers valuable insights into the interplay of factors such as perceived trust, risks, and technological prudence in shaping behavioral intentions, contributing to a deeper understanding of biometrics in a rapidly digitizing society.

Keywords Biometrics, Public attitude, Perceived trust, Perceived risk, Media governance

From voice assistants such as Siri, Alexa and XiaoAi to face recognition powered by Alipay and WeChat, biometrics has been applied in various scenarios: in real life, it is the key for users to access social services; in the scene of human-machine integration, it can be used as a supporting media technology to distinguish human objects and tell their emotions; in a metaverse scene, users' biometric information can be used as an identifier[1]. Modern biometrics has therefore reconstructed the user's Cyborg (cybernetic organism), or to say, the user's biometric information constitutes the key part of the password system[2]. By June 2023, the number of mobile Internet users in China reached 1.079 billion[3], witnessing an essential growth of users of biometrics with smart phones. Biological data usage in these contexts involves multiple potential stakeholders such as users, manufacturers, and undesirably, hackers and foreign entities. Smartphone users provide their biometric information for security and convenience, whose data was thereafter collected and stored by the manufacturers abiding by strong security measures to prevent potential unwanted access for hackers and foreign entities[4]. Hence, stringent oversight and related regulations are vital for proper usage and protection of users' biological data.

However, biometric systems remain vulnerable at the perception, network, and application layers, posing a significant threat to the security of the Internet of Things (IoT) and social networks. The current misuse of biometrics has resulted in numerous social issues, including the disclosure of personal information, excessive data demands by companies, and the proliferation of illegal deepfake technologies[5]. These problems have not only contributed to serious illegal and criminal activities but also garnered significant attention from the government, media, academia, and the public. The increasing frequency and severity of these issues underscore the urgent need for robust security measures and comprehensive governance frameworks to mitigate the risks associated with biometric systems[6]. Addressing these vulnerabilities requires technological advancements, but more critically, it necessitates an evolution in our understanding of biometrics concepts. According to McLuhan, everything is a medium[7]. Biometrics, as a medium, bears the real identity information of network users. By

[1]School of Information Management, Nanjing University, Nanjing, Jiangsu Province, China. [2]Department of Chinese and Bilingual Studies, Faculty of Humanities, The Hong Kong Polytechnic University, Hong Kong, China. [3]School of Publishing, Communication University of Zhejiang, Hangzhou, Zhejiang Province, China. ✉email: austinfreud21@gmail.com

viewing biometrics as a new medium, we can adopt a broader governance perspective, exploring human-centric and personalized strategies beyond technology. To safeguard user information security, it is imperative to conduct research on biometrics from the perspective of media governance[8], underlying three dimensions: the strengthening of civil society, the supervision from the government, and the cross-cultural consultation among international institutions and organizations. The media studies the laws and mechanisms of the communication elements within the information system and plays a supportive role at both micro level and macro level, with the aim of achieving effective media governance[9].

The current research mainly concentrates on public attitude and media governance of biometric information dissemination. Firstly, the theory of risk society is adopted to interpret the public's cognitive acceptance and risk awareness regarding the dissemination of biometric information as the factual basis for media governance[10]. Subsequently, explores the influence chain of user's perception of biometric communication and provides some possible measures for the governance of biometric information dissemination[11].

Advancements and applications in biometric technology

The roots of biometrics can be traced back to ancient times when rudimentary forms of identification based on physical traits were used. However, it was not until the 20th century that biometrics developed into an independent discipline. The publication of the first academic paper on biometrics can date back to 1963[12]. Since then, remarkable progress has been made in improving the accuracy and reliability of biometric recognition techniques under controlled environmental conditions. Technological advancements have enabled the extraction and analysis of a wide range of biometric features, including facial features, fingerprints, palm prints, iris patterns, hand geometry, handwriting styles, and voice characteristics[13]. These traits are characterized by a high degree of uniqueness. Such uniqueness endows biometrics with the capacity to act as a dependable means for identifying and differentiating individuals, much in the same way as a medium that conveys specific identity-related information[14]. Most biometric traits remain relatively stable over time, ensuring the consistency of a person's identity over an extended period, and function as a reliable medium for identity verification and information conveyance[15].

Biometrics as a medium has found wide applications in multiple fields, exemplified by security and access control. For example, fingerprint recognition is used for unlocking smartphones, granting access to secure facilities, and authorizing transactions[16]. Facial recognition is applied in banking, airports and surveillance systems for screening and identifying individuals, while iris recognition is employed to secure access in high-security areas[17]. In forensics, biometric evidence like fingerprints and DNA analysis (a molecular-level form of biometrics) helps identify suspects and build stronger cases in criminal investigations and paternity testing[18]. Moreover, in the digital realm, particularly on social media platforms and other online services, facial recognition is used for photo tagging and verifying user identity during account operations[19].

The popularization of technology has led to a wide adoption of both unimodal and multimodal biometric authentication systems[20]. The core to unimodal biometric authentication systems is a solitary biometric identifier, using fingerprint or facial recognition to verify the identity of users and thwart unauthorized access to Internet of Things (IoT) devices and services[21]. In contrast to traditional password-based authentication methods, these biometric-based systems bring greater convenience and enhanced security. Multimodal biometrics, moreover, entails the utilization of multiple biometric information sources[22]. Such systems combine biometric evidence from diverse features with the aim of augmenting recognition accuracy. Multimodal biometric systems outperform unimodal ones with notable advantages, such as higher recognition accuracy and strengthened security[23].

Recent development of artificial intelligence (AI) has brought benefits to the biometrics field with technologies such as deep learning methods. Nevertheless, several potential gaps remain to be addressed in the real-world applications of deep learning methods in biometrics[24]. These encompass the design of robust algorithms for handling biometric samples obtained from uncooperative subjects in unconstrained environments, a deeper exploration of the distinctiveness and persistency of biometric traits, measures taken to ensure biometric data security and against larger system-level concerns such as usability, user privacy, seamless integration with end applications, which can finally return on investment[25]. Therefore, an interdisciplinary research will not only facilitate the widespread adoption of biometrics as a promising technology but also enhance user acceptance with a broader societal impact.

Research on biometrics in the field of communication

In fields of communication, law, and sociology, scholars have increasingly taken biometrics as a medium or intermediary. Liu and Yu[19] proposed a biometric keys-enhanced multimedia encryption algorithm for social media blockchain. They described processes entailed such as image preprocessing, feature extraction and fusion, key generation and encryption, and evaluated its performance in key generation time, security level and encryption-decryption time complexity through simulation experiments compared to the previous ones. Shilina[26] put forward that biometrics can serve as a promising solution for restoring trust and combating misinformation within the online media realm. In her view, biometrics is capable of quantifying individuals' unique characteristics with multiple potentials of identity verification and malicious behavior counteraction.

Scholars from the field of communication mainly pay attention to the risks and ethical norms in the dissemination of biometric information. However, much of their research addresses issues of governance at a higher level, rarely promoting the construction of media governance system from a user's perspective. Sultana et al.[27] introduced social behavioral biometrics (SBB) for the first time to both real and virtual fields and discussed upon its application prospect in personal identity verification (PIV) and social interaction. Tumpa et al.[28] expounded the potential usage of behavioral biometric features such as user voice, glance, and gait, and emphasized their importance in an intelligent society. Later on, Alsaadi[29] offered a detailed summary of the major advantages and disadvantages of the most popular SBB technologies.

Upon biometric risk management, Wang[30] proposed multiple dimensions to avoid the risk of personal information dissemination based on 525 criminal adjudication documents. Lin[31] put forward the concept of "associated privacy" in biometrics, and constructed a corresponding protection mechanism. Cheng[32] believed that the profit-seeking nature of the capital market masks the potential risks of biometric communication. Gao[33] constructed a differential rule system for biometric information protection by identifying the subjects and acknowledging the dual attributes of the information. Lin and Lin[34] discussed the technical risks and multiple regulations of AI face swap based on *the Civil Code* and *the Provisions on Management of Deep Synthesis in Internet Information Service*in China. Zhang and Wang[35] believed that regulators should rely on legislation, regulatory sandboxes, and technical standards to enhance the risk management system of face recognition technology in China.

Scholars have also been widely concerned about users' acceptance and attitude towards biometrics in a voluntary context. It has been found, through a comprehensive approach built on multiple theories, that a variety of factors, such as compatibility, perceived usefulness, convenience, privacy concerns, trust in the technology, and perceived risk, exert an influence on the acceptance and recommendation of biometrics[36]. Lehto et al.[37] utilized a split-plot scenario-based experimental design and carried out a comparison of prospective travelers' attitudes towards hotel services empowered by biometrics data based on a sample size of 579 respondents in the United States. This comparison was performed both prior to and subsequent to the presentation of information concerning the risks and usage of the disclosed data….

Legislation is the cornerstone as well as a solid guarantee for the governance of biometric information dissemination. A rough dichotomy of statutory law and common law can generalize laws implemented around the world[38]. The Federal Government of the United States has issued *the Ethical Use of Face Recognition Act*, *the Commercial Facial Recognition Privacy Act* and *the Facial Recognition Technology Warrant Act*. States were given the freedom to issue independent bills for biometric technology management. On the contrary, core governance documents of the Europena Union such as *the General Data Protection Regulation* (GDPR) and *the EU Artificial Intelligence Act*, are characterized by overarching supervision[39].

To sum up, extensive research efforts have been centered on both the applications and potential negative impacts of biometrics, with particular attention paid to issues regarding privacy, security, as well as ethical norms. These studies strived for an understanding of how biometric technologies influence social structures, legal frameworks, and communication practices by meticulously focusing on the far-reaching implications brought about by the application of biometrics. Existent studies emphasized the necessity of implementing stringent regulation and oversight mechanisms for alleviation and minimization of the adverse consequences that may arise from the utilization of biometrics.

At present, the main concern of biometric information dissemination focuses on the protection of personal data. The abuse, tampering and leakage of personal and corporate data have triggered public concern about technical risks. The updates of legislation often fail to follow the iteration of new technologies notwithstanding its place as the most effective way of social governance. For example, China's *Data Security Law*was officially implemented on Sept. 1st, 2021. In 2023, when Big Data Research Institute of Southern Metropolis Daily investigated the public's perception of the results after its promulgation, more than half of the respondents were still reported to worry about how they could protect their rights after data leakage[40]. Therefore, theoretical basis is needed in research for data governance with a forward-looking vision and risk management awareness.

Research methodology

Theoretical framework

The theory of Risk Society holds that risk is a social reality in the era of globalization[41]. Zhang[42] believed that in the digital age, this theory applies the idea of risk control to a constructive interpretation of social norms and plays a role in stopping risks before they grow, thereby reducing technological uncertainty and possible undesirable consequences. Based on the Technology Acceptance Model (TAM), Diffusion of Innovations theory (DOI), and Unified Technology Acceptance and Use Theory (UTAUT), Caroline et al. synthesized the variables in the DOI, TAM, and UTAUT models in their work. Additionally, they took specific factors such as perceived risk, trust, privacy concerns, and innovation into account. The study discovered that, aside from innovation, the most crucial drivers explaining the acceptance and recommendation of biometrics stem from trust and privacy protection rather than elements in traditional acceptance models[36]. However, the current study only focused on one type of biometric system, namely iris scanning, while the inclusion of different types of biometrics might be confusing and may lead to different results. Simultaneously, the sample size and age range are limited, and their study did not include the elderly group, which may drastically impact the results. On this basis, this study incorporated more biometric types into investigation and constructed a new structural equation model (SEM) with an expanded sample size.

In our study, five major factors were included:

(1) Perceived availability.

In the present study, perceived availability is incorporated into our framework as an individual's subjective assessment of the facility with which they can access and utilize biometric technology services. It often addresses users' perceptions of the accessibility of technological tools, digital content, or support systems[43]. It is distinct from actual availability, emphasizing the psychological and situational factors that shape perceptions rather than objective conditions[44–46].

(2) Perceived trust.

Within the realm of communication, perceived trust is incorporated into our framework as an individual's subjective conviction or confidence regarding the reliability, integrity, and competence of biometric technology services. In the cognitive dimension, trust is grounded in an evaluation of an entity's attributes, including trustworthiness, expertise, and predictability. On the emotional level, trust encompasses a sense of security and confidence within a relationship or interaction. Furthermore, perceived trust can vary significantly across different contexts, such as e-commerce[47], information technology acceptance[48] and Internet relationships[49].

(3) Perceived risks.

In the field of communication, perceived risks are included in our framework as an individual's subjective evaluation of potential negative outcomes or uncertainties associated with biometric technology services[52–55].

(4) Perceived attitudes.

In the current study, the dichotomy of technological optimism/prudence constructed the binary nature of perceived attitudes of biometrics[53]. Technological optimism is the belief that technology will bring about positive societal change, improve quality of life, and resolve complex global challenges.Individuals with this orientation generally perceive technological advancements as beneficial and view them as key drivers of economic growth, social progress, and innovation[46–54].While technological prudence is included as a more cautious, skeptical, or risk-averse stance toward technology of people[56]. Individuals or groups exhibiting technical prudence are concerned about the potential risks and negative consequences of technological advancements, such as privacy violations, job displacement, or environmental harm[57]. Technical prudence is associated with a critical view of technology, emphasizing the need for regulation, ethical considerations, and the careful evaluation of risks before widespread adoption. A more cautious approach is evident in discussions about AI ethics, data privacy, and the environmental impact of emerging technologies[58].

(5) Behavioral intention.

Behavioral intention refers to an individual's planned or intended behavior, often measured in the context of adopting new technologies or engaging with systems[59]. In the field of biometric systems, behavioral intention involves users' willingness to use or interact with biometric authentication methods[60–66] based on their perceived ease of use, trust, and security concerns. It plays a key role in predicting actual usage behavior, such as adopting biometric technologies for security or identification purposes.

The questionnaire design (see Sect. 4.3) in the current study is based on the modification of three essential documents, i.e., *the 2020 National Survey of Civic Scientific Literacy in China*[67], *Awareness, Acceptance and Willingness to Buy Genetically Modified Foods in Urban China*[68], and *Provisions on Security Management in the Application of Facial Recognition Technology (Trial) (Draft for Comment)*[69]. This study begins by proposing a series of research questions and hypotheses aimed at understanding the public's perceptions and attitudes toward biometrics. Specifically, it investigates the relationship of perceived availability (PA), perceived trust (PT), perceived risks (PR), technological optimism (TOp), technological prudence (TP), and behavioral intentions (BI) to biometric information.

Research questions and hypotheses

Based on the framework illustrated in the previous section, we propose four research questions (RQs) for the current study:

RQ1: Does the availability of biometric technologies bring about perceived trust (PT) or perceived risks (PR) in the public?

RQ2: How and to what extent do the public's perceived trust (PT) and perceived risk (PR) of technology affect the use and popularity of biometrics (BI)?

RQ3: How will the public's different emotional attitudes towards biometrics (technological optimism, TOp, or technological prudence, TP) affect the behavioral intention (BI) of public?

RQ4: What are the possible measures to be taken to increase public trust (PT) in technology and effectively manage the risks (PR) associated with the dissemination of biometric information?

Accordingly, six research hypotheses (RHs) are raised as follows:

Previous studies have highlighted that familiarity with and ease of access to biometric technologies play a crucial role in enhancing public trust. For instance, Miltgen et al.[36] demonstrated that perceived usefulness and ease of use positively correlate with users' trust in such technologies. As biometrics have become increasingly embedded in everyday activities, their usefulness is widely recognized and self-evident. Consequently, this study employs the variable of perceived availability (PA) to better capture people's perceptions of biometric technologies.

RH1: The perceived availability (PA) of biometric technologies positively influences perceived trust (PT) in these technologies.

While increased availability fosters trust, it simultaneously raises awareness of potential risks. As Miltgen et al.[36] noted, the increased exposure to biometric systems can lead to heightened privacy concerns and perceived risks due to frequent media coverage on data breaches and misuse.

RH2: The perceived availability (PA) of biometric technologies positively impacts perceived risks (PR) associated with their use.

Trust in technology has been identified as a significant driver for its adoption. The trust model highlights that higher levels of trust lead to a stronger willingness to adopt and recommend biometric systems, particularly when users perceive minimal privacy infringement[70].

RH3: Perceived trust (PT) in biometric technologies positively affects behavioral intention (BI) to use these technologies.

Perceived risks, especially those related to privacy and data security, are critical deterrents for technology adoption[51]. Empirical evidence suggests that users are hesitant to adopt biometric technologies when they associate them with potential risks of misuse or unauthorized access[52].

RH4: Perceived risks (PR) of biometric technologies negatively affect the behavioral intention (BI) to use these technologies.

Technological optimism is often linked to high levels of trust in technological solutions and a willingness to embrace new technologies, particularly in domains such as healthcare, education, and sustainability[55]. Optimistic attitudes towards technology can mitigate concerns over risks and enhance behavioral intentions. Miltgen et al.[36] identified optimism as a mediator that reduces the psychological barriers associated with adopting disruptive innovations like biometrics.

RH5: Technological optimism (TOp) positively influence the behavioral intention (BI) to use biometric technologies.

While prudence can protect users from potential risks, excessive caution may limit their willingness to engage with emerging technologies. According to Miltgen et al.[36], prudent users are less likely to adopt biometric systems due to amplified concerns over data protection.

RH6: Technical prudence (TP) negatively affect the behavioral intention (BI) to use biometric technologies.

Questionnaire design and data collection

The questionnaire used in the current study is listed as Table 1. The significance of this questionnaire lies in its role in developing a comprehensive scale to examine the public's perception, trust, risk awareness, emotional attitudes toward the technology, and behavioral intentions regarding the dissemination of biometric information. This study aims to identify user-related factors and, building on existing theories, propose enhanced strategies to effectively manage the risks associated with biometric information dissemination.

The questionnaire was designed and distributed via the online survey platform Wenjuanxing (www.wjx.cn). The platform was chosen for its widespread usage and robust data management features, which facilitated efficient distribution and collection. The survey included questions assessing participants' perceptions, trust, risk awareness, emotional attitudes, and behavioral intentions regarding biometric information dissemination. A financial incentive of 5 CNY was offered to each participant upon successful completion of the survey, significantly enhancing the response rate.

This study adhered strictly to the ethical guidelines outlined in the Declaration of Helsinki and was approved by the Science and Ethics Committee at University of Chinese Academy of Sciences (UCAS). All procedures complied with relevant regulations, and informed consent was obtained from all participants before the survey. To ensure privacy, personal identities were anonymized during data collection and throughout the data analysis process.

Participants were recruited through multiple online channels, including social media platforms (Xiaohongshu and Weibo), community groups (WeChat groups), and email lists. This ensured a diverse demographic representation. To maximize participation, the survey link was accompanied by a clear introduction outlining the research purpose, confidentiality assurances, and details about the monetary reward.

A total of 2,000 questionnaires were distributed. Responses were monitored in real-time to track progress and detect anomalies. By the end of the data collection period, 1,913 responses were received, yielding a response rate of approximately 96%.

Upon completion of the data collection, the responses underwent a rigorous three-step screening process to ensure data quality: Firstly, incomplete questionnaires were automatically flagged and excluded; secondly,

Variable factor	Items(Items 1 to 7 of the questionnaire are demographic information.)
Perceived availability	(8)You've heard about face recognition, fingerprint recognition, etc. (9)You have used or are using face recognition, fingerprint recognition and other technologies. (10)You know the term "biometrics." (11)We use biometrics every day without even realizing it.
Perceived trust	(12)Biometrics technology has strong security. (14)Biometrics technology brings a lot of convenience to our life. (16)Biometrics protect our personal and property security. (18)The use of biometrics does not harm the human body.
Perceived risks	(13)Biometrics can lead to leakage of personal information. (15)Biometrics can lead to financial fraud, deep counterfeiting and other risks. (17)Biometrics violate our personal and property security. (19)The use of biometrics can cause harm to the human body.
Technological optimism	(20)You accept the use of computer technology by a state or business to extract and process physiological or behavioral characteristics inherent in the human body for personal identification. (21)You support the country and society to widely use biometrics in the fields of national security, public security, criminal investigation and justice, mobile payment and finance.
Technical prudence	(22)You are concerned about illegal access, copying, disclosure, external provision, dissemination of personal images and other behaviors. (23)You are worried about personal information disclosure, tampering, loss, or illegal acquisition, illegal use, etc. (24)You have heard of or encountered situations where individuals have been coerced, misled, defrauded, or coerced into accepting facial recognition technology to verify their personal identity. (25)You are concerned that facial recognition technology is used to analyze sensitive personal information such as an individual's race, ethnicity, religious beliefs, health status, social class, etc.
behavioral intention	(26)Encounter illegal use of biometrics, you can find and report to the relevant departments in a timely manner. (27)Within the safe limits, you accept and use face recognition technology[60]. (28)Within the security limits, you accept and use fingerprint recognition technology[61]. (29)Within the safe limits, you accept and use palmprint recognition technology[62]. (30)Within the safe limits, you accept and use iris recognition technology[63]. (31)Within the safe limits, you accept and use hand recognition technology[64]. (32)Within the bounds of security, you accept and use signature recognition technology[65]. (33)Within the safe limits, you accept and use voice recognition technology[66].

Table 1. Measurement variables and Questionnaire Item table (translated from Chinese).

responses completed in an unreasonably short time were considered invalid, as they likely did not reflect genuine engagement; thirdly, surveys exhibiting clear response patterns (e.g., selecting the same option for all questions) were discarded.

In the end, this screening process resulted in 1,862 valid responses, with a validity rate of about 97%.

Data analysis and results

Descriptive statistics of participant profiles

As shown in Table 2, responses to this public survey features remarkable diversity across demographic and socio-economic dimensions, ensuring a comprehensive and inclusive representation. Gender balance is nearly achieved, with male participants accounting for 51.1% and females representing 48.9%. Additionally, the sample highlights cultural diversity, as 90.0% of the participants are Han Chinese, while 10.0% come from ethnic minority groups.

The participants also reflect an even distribution between urban and rural areas, with 50.9% identified as urban residents and 49.1% as rural residents. Age diversity is notable, spanning from individuals under 18 years old (7.7%) to those over 70 years old (3.4%). The largest age group is 18–29 years (26.1%), followed by 30–39 years (19.0%), ensuring perspectives from different stages of life.

Geographically, the sample captures a wide range of regional perspectives, with participants from Eastern China (32.7%), Central China (41.6%), and Western China (25.7%). Educational backgrounds are equally diverse, ranging from primary school and below (13.2%) to postgraduate and above (12.0%). A significant proportion of participants hold junior school (21.2%) or graduate (20.4%) qualifications, illustrating a broad spectrum of educational attainment.

Occupational diversity is another strength of the sample. Participants represent a variety of professional and personal backgrounds, including state organ staff (8.9%), professionals and technical personnel (12.7%), students (13.5%), and workers across agriculture, commercial, and service sectors. Additionally, a notable proportion of participants are retired (8.7%), unemployed (6.4%), or domestic workers (6.2%).

This broad diversity across gender, ethnicity, residency, age, region, education, and occupation underscores the robustness of the participant groups, providing rich and varied perspectives for the study.

Table 3 offered a descriptive account of the constructs measured in the questionnaire, as shown below.

Table 4 demonstrated the results of correlation analysis between different constructs. In case that some of the variables may not be normally distributed, Spearman's rank correlation analysis was adopted in this case. The correlation coefficients and corresponding significance level are listed below.

The correlations between variables in the Table 4 illustrates an interwoven network among multiple variables. For instance, PA not only directly affects PT and BI but is also related to PR, TOp, and TP. Similarly, PT exhibits significant relationships with PR, TOp, TP, and BI. This complex network of relationships suggests that public attitudes toward biometric technology constitute a multidimensional and interdependent system, where the influence of a single variable on public attitudes cannot be viewed in isolation.

Model construction

In this study, IBM SPSS Statistics 24.0 and AMOS 24.0 were used for data processing and structural equation model construction. Relationships among perceived availability (PA), perceived trust (PT), perceived risks

Item	Options	Count	Proportion (%)	Item	Options	Count	Proportion (%)
Gender	Male	951	51.1	Education Level	Primary school and below	246	13.2
	Female	911	48.9		Junior school	394	21.2
Nationality	Han	1,675	90.0		High school or secondary vocational school	382	20.5
	Ethnic minorities	187	10.0		Three-year college	238	12.8
Household Registration	Urban resident	948	50.9		Graduate	379	20.4
	Rural resident	914	49.1		Postgraduate students and above	223	12.0
Age	Under 18 years old	144	7.7	Occupation	Staff of state organs and party-mass organizations	166	8.9
	18–29 years old	486	26.1		Person in charge of enterprises and public institutions	137	7.4
	30–39 years old	353	19.0		Professional and technical personnel	236	12.7
	40–49 years old	292	15.7		Office staff	209	11.2
	50–59 years old	271	14.6		Production personnel of agriculture, forestry, animal husbandry, fisheries and water conservancy	147	7.9
	60–69 years old	253	13.6		Workers in the commercial and service sectors	142	7.6
	Over 70 years old	63	3.4		Operators of equipment production and transportation	122	6.6
Region	Eastern China	609	32.7		Students and those awaiting admission	252	13.5
	Central China	775	41.6		Unemployed and laid-off workers	119	6.4
	Western China	478	25.7		Retired and former workers	162	8.7
					Domestic workers	116	6.2
					Other	54	2.9

Table 2. Descriptive statistics of samples.

Var.	Mean	Median	SD	Min	Q1	Q3	Max	Skewness	Kurtosis
PA	3.895	4.25	1.006	1	3.75	4.5	5	−1.246	0.623
PT	3.824	4	0.987	1	3.5	4.5	5	−1.112	0.377
PR	3.746	4	1.014	1	3.25	4.5	5	−1.027	0.086
TOp	3.876	4	1.064	1	3.5	4.5	5	−1.106	0.425
TP	3.925	4.25	0.989	1	3.75	4.5	5	−1.361	0.948
BI	3.828	4.125	0.996	1.125	3.625	4.5	5	−1.201	0.274

Table 3. Descriptive statistics of variables in responses.

	PA	PT	PR	TOp	TP	BI
PA	1					
PT	0.577	1				
PR	0.465	0.622	1			
TOp	0.402	0.533	0.622	1		
TP	0.402	0.404	0.43	0.49	1	
BI	0.455	0.488	0.443	0.506	0.454	1

Table 4. Spearman's rank correlation between variables. *** $p < 0.001$.

(PR), technological optimism (TOp), technical prudence (TP), and behavioral intention (BI) to use biometric technologies were examined. Drawing from previous studies and the theoretical foundation, this study integrates variables that capture both enabling and deterring factors in the adoption of biometric technologies.

The structural equation model (SEM), illustrated in Fig. 1, visualizes the hypothesized relationships and their corresponding items measured[71]. Each latent construct is measured by multiple observed variables, ensuring robust analysis through confirmatory factor analysis (CFA) and path modeling.

To assess the reliability and validity of the measurement model, we examined the factor loadings, average variance extracted (AVE), composite reliability (CR), and Cronbach's alpha for each construct. The results, summarized in Table 5, indicate that the measurement model exhibits satisfactory reliability and validity.

Factor loadings, Average Variance Extracted (AVE), Composite Reliability (CR), and Cronbach's α are critical indicators in SEM for the assessment of the model quality.

In this study, the factor loadings (all greater than 0.5) indicate strong correlations between the indicators and their corresponding latent variables, suggesting that the indicators adequately represent the latent variables. A higher AVE implies that the latent variable explains a larger proportion of the variance in its indicators, reflecting better convergent validity. The AVE values for the variables in this study are all above 0.5, demonstrating good convergent validity—the indicators effectively capture the common characteristics of the latent variables. Higher CR values indicate stronger correlations among the indicators. In this study, the CR values for all variables exceed 0.7, showing good internal consistency, i.e., the indicators consistently measure the latent variables. Cronbach's α, which ranges from 0 to 1, measures the internal consistency of indicators, with higher values indicating better reliability. Generally, an threshold of 0.7 is considered acceptable. Accordingly, the Cronbach's α values for all variables in this study meet this criterion. A conclusion of good overall fit of the SEM model can be drawn from parameters in Table 6.

Table 7 shows path coefficients between variables included in the SEM model. Discerned from the standardized coefficients, PA is the most important factor influencing PT. Both TP and PA have significant impacts on PR, with TP exerting a greater influence. Regarding factors influencing BI, PT ranks among the most influential ones, followed by TP, while PR has a negative and more moderate effect.

The results of this study confirm the positive influence of perceived availability and trust on behavioral intention, while also highlighting the significant deterrent effect of perceived risks. Although the relationship between perceived availability and perceived risks (RH2) and the impact of technological optimism (RH5) were not explicitly tested, the findings provide robust support for the hypothesized effects of availability and trust. Interestingly, the analysis revealed an unexpected positive relationship between technical prudence and behavioral intention, challenging the initial hypothesis (RH6) and suggesting a more nuanced dynamic where cautious users may still adopt biometric technologies if they perceive them as secure and trustworthy. These findings contribute to a deeper understanding of the factors driving the adoption of biometric systems, underscoring the critical roles of trust, risk mitigation, and user confidence in shaping behavioral intentions.

Governance measures for biometrics as a media in the digital Intelligence Era

Biometric information differs significantly from ordinary privacy information, as it encompasses not only personal and property safety but also the broader implications for the future order of information dissemination. Unlike conventional privacy concerns, biometric data involves risks that extend beyond privacy, including potential irreversible harm that could profoundly impact both individuals and society. The nature of biometrics prevents us from focusing merely on the surface of privacy risk control. The public must recognize and address

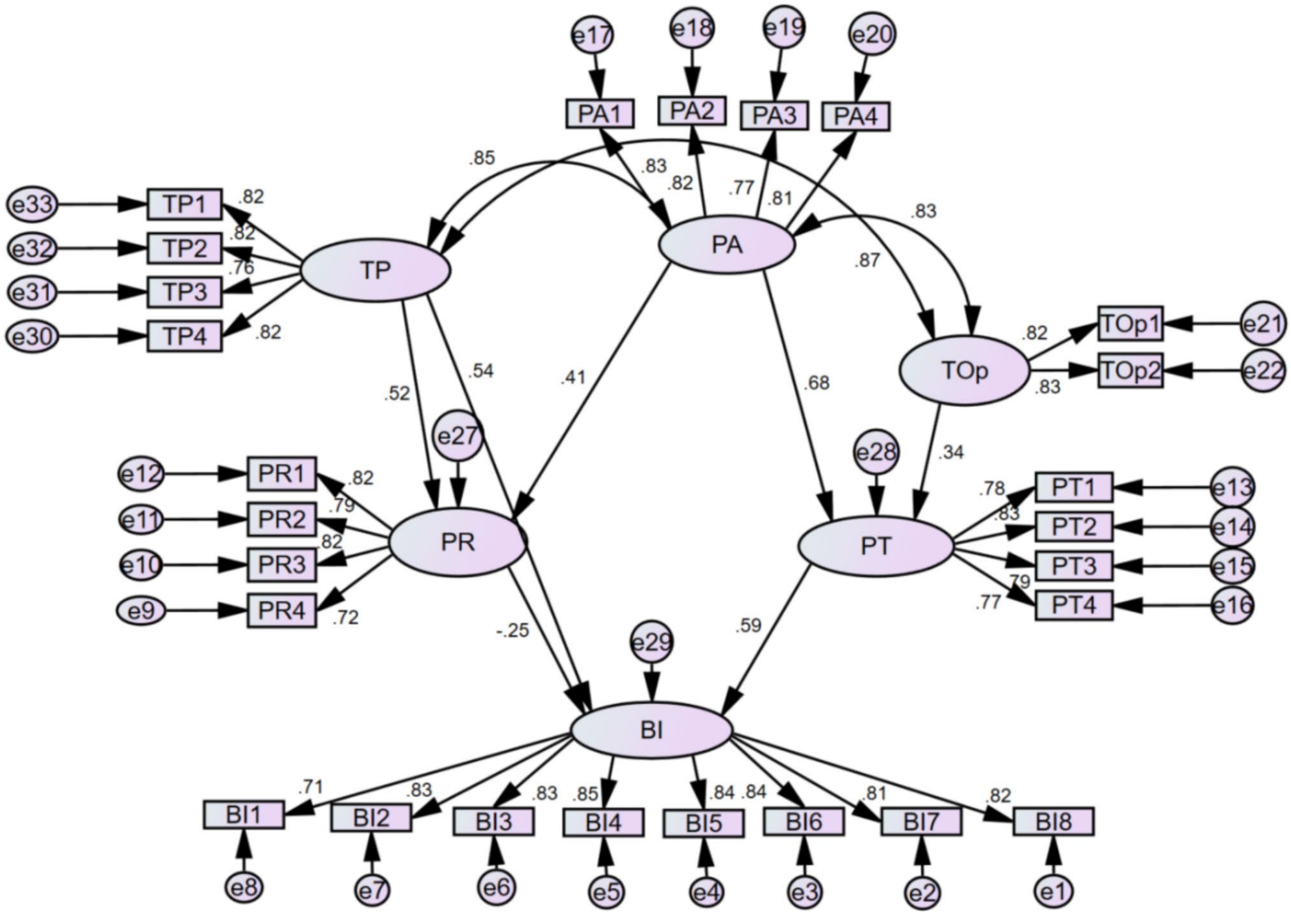

Fig. 1. Structural equation model diagram.

potential financial, social, and virtual risks underneath, while improving digital literacy to navigate the challenges of deep media ecosystems and the emerging metaverse.

Findings from this study underscore the critical role of trust and risk perception in shaping behavioral intentions toward biometric technologies, aligning with the need to mitigate risks and foster trust we are talking about. The construction of trust requires a multifaceted approach that not only ensures privacy protection but also addresses broader systemic risks. In the first place, governments should play a leading role by fostering collaboration among mass media, academic scholars, and enterprises. The establishment of specialized legal frameworks, dissemination of knowledge, and development of targeted technologies to address vulnerabilities can cultivate cross-sectoral partnerships to tackle the inherent challenges to this topic. This comprehensive approach symbolized the inner demand of results from the current study, which emphasize the role of trust-building and risk mitigation to promote the adoption of biometric technologies and ensure their responsible integration into the social fabric.

Enhancing public trust in biometric technologies through legislation

The norms and ethics in communication have been undergoing a process of dynamic development with the changing media environment. Various countries have issued relevant laws and regulations for the dissemination of biometric information, but there are still cases of misappropriation, disclosure and abuses, as well as ethical problems of discrimination. Currently, China's legislation on facial information protection remains incomplete and requires significant improvement. On May 1st, 2021, the Cyberspace Administration of China reported that 33 social apps, navigation apps, and input method editors (IME) were found of illegal collection and abuse of personal information. There is also an illegal industrial chain of face verification where outlaws trade videos containing ID photos or other face information to skip the identity verification steps of online platforms and access control systems, thus undermining others' property and privacy[72].

Increasing public trust in biometrics through legislation requires a comprehensive and thoughtful approach that addresses the unique privacy, security, and ethical concerns associated with biometric technologies[73]. First, explicit privacy protections should not only define how biometric data can be collected, stored, processed, and shared but also address emerging technologies such as AI-driven biometric analysis[74]. These provisions must include dynamic consent mechanisms, allowing users to update or withdraw consent as the contexts in which the data is used evolve. Additionally, data minimization policies should explicitly incorporate assessments to ensure corporate compliance— organizations should justify the necessity of the data collected for specific purposes.

Factor	Items	Loadings	t	AVE	CR	Cronbach's α
PT	PT1	0.78	39.57	0.62	0.81	0.77
	PT2	0.83	41.19			
	PT3	0.79	37.58			
	PT4	0.77	36.08			
PR	PR1	0.82	33.77	0.71	0.92	0.89
	PR2	0.79	32.65			
	PR3	0.82	33.64			
	PR4	0.72	27.2			
BI	BI1	0.71	34.81	0.65	0.93	0.91
	BI2	0.83	43.14			
	BI3	0.85	44.23			
	BI4	0.84	42.51			
	BI5	0.84	42.5			
	BI6	0.81	41.13			
	BI7	0.82	41.42			
	BI8	0.82	40.14			
TP	TP1	0.82	41.37	0.68	0.91	0.89
	TP2	0.82	41.1			
	TP3	0.83	37.26			
	TP4	0.82	38.88			
PA	PA1	0.83	42.51	0.70	0.89	0.87
	PA2	0.82	42.02			
	PA3	0.77	38.92			
	PA4	0.81	42.04			
TOp	TOp1	0.82	39.88	0.67	0.88	0.88
	TOp2	0.83	39.8			

Table 5. Factor loadings, AVE, CR, and Cronbach's *α*.

Fit Index	Value	Acceptable Threshold	Threshold of Good Fit	Degree of Fit
χ^2/df	6.035	2–3	< 2	Acceptable
GFI	0.925	0.7–0.9	≥ 0.9	Good
RMSEA	0.052	0.05–0.08	≤ 0.05	Acceptable
AGFI	0.908	0.7–0.9	≥ 0.9	Good
IFI	0.963	0.7–0.9	≥ 0.9	Good
CFI	0.963	0.7–0.9	≥ 0.9	Good
NFI	0.956	0.7–0.9	≥ 0.9	Good

Table 6. Model Fit statistics.

Path	Estimate Coeff.	S.E.	C.R.	Sig. Lvl.	Standardized Coeff.
PT <-- PA	0.652	0.032	20.393	***	0.679
PT <-- TOp	0.324	0.030	10.851	***	0.339
PR <-- TP	0.519	0.040	13.074	***	0.517
PR <-- PA	0.406	0.038	10.823	***	0.414
BI <-- PR	−0.260	0.046	−5.703	***	−0.245
BI <-- PT	0.638	0.047	13.707	***	0.589
BI <-- TP	0.579	0.052	11.197	***	0.545

Table 7. Path coefficients between variables. *** $p < 0.001$.

To strengthen data security requirements, encryption standards must align with best global practices, such as quantum-resistant cryptography, to prevent biometric data against emerging threats. Organizations that breach these standards should be obligated to provide remediation support, such as identity theft protection, to affected individuals. Independent audits must also evaluate the ethical implications of biometric systems alongside security compliance to address broader societal impacts. Moreover, incorporating best global practices requires an international consensus on biometric data governance, especially in contexts like cross-border data sharing. Legislation should actively engage with international organizations to harmonize standards and address jurisdictional conflicts[75]. Finally, implementing adaptive and forward-looking policies requires the establishment of a dedicated advisory body to review and recommend legislative updates in response to technological advancements. Additionally, innovative patterns exemplified by sandbox regulations should incorporate clear criteria for the transition period through the full-scale deployment of tested technologies, ensuring accountability and minimizing risks during the scaling process.

Ensuring ethical use and fairness of biometrics necessitates mandatory periodic assessments of biometric algorithms for bias and discrimination, particularly in high-stake scenarios such as law enforcement and employment. Strict prohibitions on misuse should include enforcement frameworks with significant penalties to deter unauthorized surveillance and data exploitation. Moreover, promoting public awareness and education should involve multi-stakeholder partnerships to create tailored educational programs addressing diverse demographic needs and literacy levels, with a focus on empowering marginalized groups. Furthermore, a more granular approach is in need for enhancing user rights. For example, individuals' right to opt-out should guarantee their access to comparable alternatives for biometric systems. Their right to opt for data erasure should be strengthened by incorporating mechanisms to verify data deletion, thereby fostering user confidence in data compliance. Oversight mechanisms should integrate real-time monitoring technologies to identify and address regulatory breaches, and transparently report detailed accountability metrics and independent verification to build public trust.

Monitoring the communication environment for lowering data leakage risk

Monitoring the communication environment is essential for reducing the risks associated with bioinformatics leakage, particularly in mitigating the threats posed by deepfakes and unauthorized dissemination of biometric data. Advanced surveillance mechanisms incorporating machine learning algorithms and digital watermarks can analyze biometric meta-information (e.g., voice and facial features) to detect anomalies and authenticate users. The implementation of these systems can help stakeholders, such as digital platforms and government agencies, collaboratively address the spread of falsified biometric information to safeguard personal and property rights. Additionally, technologies like sound anomaly recognition, when carefully deployed, can ensure the ethical use of biometric data for specific purposes, such as safety and environmental monitoring, while preventing misuse in precision marketing and unauthorized surveillance.

Robust monitoring mechanisms also address broader algorithmic and privacy risks by overseeing how biometric data is processed and utilized by enterprises. This includes establishing regulations for the systematic evaluation of biometric data to prevent its exploitation as a commercial asset and addressing practices that contribute to pervasive surveillance environments, such as the concept of the "super-panopticon."[76] Real-time monitoring systems act as effective early warning mechanisms, capable of detecting data breaches, anomalies, and unauthorized data flows, enabling rapid intervention to mitigate potential damage before it escalates. These measures not only mitigate the risks of biometric information leakage but also strengthen public trust in biometric technologies by promoting accountability and transparency among data operators.

Furthermore, monitoring mechanisms play a critical role in identifying and mitigating the "invisible harm" associated with biometric communication, where users unknowingly become subjects of data manipulation, thereby losing their autonomy[77]. By highlighting algorithms that predict and exploit user behavior without consent, monitoring mechanisms ensure users of the right for control over their biometric data. At the same time, the mechanisms promote the ethical use of technology and mitigate the societal risks of technology dependence, where individuals passively accept privacy invasions and technological manipulation. Coupled with efforts to enhance digital literacy and ethical governance, monitoring systems contribute to a safer and more equitable communication environment in the era of digital intelligence[78].

Towards a governance framework of balanced availability and security of biometrics

To address public perception and risk awareness issues of biometric technologies, policymakers should prioritize enhancing regulation transparency, promoting ethical standards, and ensuring balanced governance. It is essential to establish robust regulations for data utilization, dissemination, and sharing, with clearly defined "thresholds" and "barriers" to prevent unauthorized collection and misuse of personal biometric information. Transparent algorithms should be mandated by regulation for enterprises to disclose decision-making processes and eliminate AI biases in exploiting biometric data, thus curtailing misuse for the construction of public trust in biometric systems.

Governance frameworks must strike a balance between accessibility and information security by integrating public and private interests[79]. Data governance should delineate clear boundaries between public and private data usage, ensuring technological advancements align with public welfare, while safeguarding individual privacy. A real-time monitoring system, with support from independent regulatory authorities, can detect and mitigate misuse as an effective early warning mechanism. Moreover, mandating external audits of data handling practices and fostering cross-sector collaboration between governments, enterprises, and independent organizations ensures accountability and promotes sustainable innovation in biometric applications[80].

The media, apart from stakeholders such as governments and enterprises, plays a pivotal role in fostering public awareness and mediating public trust. Serving as an intermediary between technology and society, the media should advocate for algorithm transparency, publicize risks associated with biometric systems, and hold data operators accountable for ethical lapses. By facilitating dialogue within the "technology-media-society" loop, the media plays a crucial role in promoting informed public discourse. Moreover, it harnesses a supervisory role as the 'Fourth Estate'[81], ensuring data governance serves social interests and maintains a balanced dynamic between technology accessibility and security. This approach not only alleviates power imbalances but also bolsters social cohesion and trust in the digital intelligence era.

Conclusion and future prospects

In the era of digital intelligence, biometrics has emerged as a pivotal technology with profound implications for personal privacy, social trust, and governance frameworks. This study systematically explored the factors influencing public perception, technology acceptance, and risk awareness of biometric technologies, while offering three possible governance measures for addressing critical challenges of balancing technology accessibility and information security. By identifying key influence chains for publics' behaviour intentions and highlighting the role of regulation transparency and collaboration among stakeholders, the current research provides a preliminary framework for enhancing public trust and mitigating risks regarding the adoption of biometric systems.

Findings from this study underscore the importance of transparent algorithms, robust data governance mechanisms, and media accountability in fostering a fair and secure communication environment. Equally crucial is the role of policymakers in delineating public-private boundaries, ensuring sustainable technological development, and addressing the structural power imbalances inherent in a data-centric society. Through proactive governance and ethical oversight, biometric technologies can be leveraged not only to optimize societal functioning but also to uphold individual rights and public trust. This study contributes to the broader discourse on digital governance, offering theoretical and practical insights that bridge the gap between technology and society. Strategies and governance frameworks proposed in this study from an interdisciplinary view may benefit a more equitable and intelligent digital future.

Key areas for future research include conducting in-depth investigations into the public's perception and acceptance of biometric technologies across different cultural backgrounds and age groups. Cultural factors can significantly shape attitudes toward new technologies. Comparative studies across different regions will provide a more comprehensive picture of these influence mechanisms. Research on the group of elderly people warrants further exploration. Given the significant differences in technological acceptance and conception of privacy between the elderly and other age groups, understanding their attitudes towards biometric technologies is crucial and meaningful for promoting customized applications for this group, hence ensuring a more balanced technological integration within society.

Additionally, following research may focus on how public perception and acceptance evolve when biometric technologies are integrated with other emerging technologies, such as AI and blockchain, to help anticipate and address potential public concerns. In certain high-security contexts, such as classified units and core financial services, the public's acceptance and trust in biometric technologies may be more complex. In-depth research in these areas can provide a foundation for developing tailored technological applications and management strategies.

Data availability

The datasets analyzed during the current study are not publicly available due to containing personal information but are available from the corresponding author upon reasonable request.

Received: 4 September 2024; Accepted: 13 January 2025
Published online: 18 January 2025

References

1. Olade, I., Fleming, C. & Hai-Ning Liang. BioMove: biometric user identification from human kinesiological movements for virtual reality systems. *Sensors* **20** (10), 2944. https://doi.org/10.3390/s20102944 (2020).
2. Yang, C. & Ren, Y. Potency and path on the Incarnate transmission in Digital Times. *Jianghan Tribune*. **8**, 15–22 (2023).
3. CNNIC. The 52nd Statistical Report on the Development of the Internet in China. (2023).
4. Kwon, H. & Lee, M. Comments on PassBio: privacy-preserving user-centric biometric authentication. *IEEE Trans. Inf. Forensics Secur.* **17**, 2816–2817. https://doi.org/10.1109/TIFS.2022.3195380 (2022).
5. Yu, Y. et al. Deepfake face tampering video detection method based on non-critical masks and attention mechanism. *Ji Suan Ji Ke Xue*. **50** (11), 160 (2023).
6. Lien, C. & Vhaduri, S. Challenges and opportunities of Biometric user authentication in the age of IoT: a Survey. *ACM Comput. Surveys*. **56**, 1–37 (2024).
7. Logan, R. K. *Understanding new Media: Extending Marshall McLuhan* (Peter Lang, 2010).
8. Seán, O. S., Girard, B. & Mahan, A. *Global Media Governance: A Beginner's Guide*12 (Rowman and Littlefield, 2002).
9. Ren, Y., Wang, H. & Embedded Scene, collaboration, and Effect: the practical approaches to the sinicization of Media Governance in the Meta-Technological Perspective. *Mod. Communication (Journal Communication Univ. China)*. **4**, 58–62 (2023).
10. Li, G. Unbalance and consciousness: theoretical source tracing of and real appeal to Risk Society. *Gansu Social Sci.* **4**, 168–177 (2023).
11. Shen, C. On the paradigm of Functionalism in Chinese Civil Law Science. *Law Social Dev.* **5**, 146–166 (2023).
12. Trauring, M. Automatic comparison of finger-ridge patterns. *Nature* **197** (4871), 938–940 (1963).
13. Jain, A. K., Nandakumar, K. & Ross, A. 50 years of biometric research: accomplishments, challenges, and opportunities. *Pattern Recognit. Lett.* **79**, 80–105. https://doi.org/10.1016/j.patrec.2015.12.013 (2016).
14. Tistarelli, M. & Champod, C. In Tistarelli M., Tistarelli M. and Champod C.(Eds.), Handbook of biometrics for forensic science (1;1st 2017; ed.). Springer Nature. (2017). https://doi.org/10.1007/978-3-319-50673-9

15. Liebers, J., Burschik, C., Gruenefeld, U. & Schneegass, S. Exploring the stability of behavioral biometrics in virtual reality in a remote field study: Towards implicit and continuous user identification through body movements. In *Proceedings of the 29th ACM Symposium on Virtual Reality Software and Technology* (pp. 1–12). (2023), October.
16. Rayani, P. K. & Changder, S. Continuous user authentication on smartphone via behavioral biometrics: a survey. *Multimedia Tools Appl.* **82** (2), 1633–1667 (2023).
17. Adewale, A. A., Ibidunni, A. S., Badejo, J. A., Odu, T. & Adoghe, A. U. Biometric enabled E-banking in Nigeria: Management and customers' perspectives. In Information and knowledge management (Vol. 4, pp. 23–28). (2014).
18. Trokielewicz, M., Maciejewicz, P. & Czajka, A. Post-mortem iris biometrics – field, applications and methods. *Forensic Sci. Int.* **365**, 112293. https://doi.org/10.1016/j.forsciint.2024.112293 (2024).
19. Liu, T. & Yu, Z. A biometric key-enhanced multimedia encryption algorithm for social media blockchain. *J. Circuits Syst. Computers*. **33** (11). https://doi.org/10.1142/S0218126624501937 (2024).
20. Oloyede, M. O. & Hancke, G. P. Unimodal and multimodal biometric sensing systems: a review. *IEEE Access.* **4**, 7532–7555 (2016).
21. Yang, W. et al. Biometrics for internet-of-things security: a review. *Sensors* **21**, 6163 (2021).
22. Yang, H., Sun, E., Cheng, C. & Ding, A. H. Multi-modal biometrics based on data fusion. *Journal of Physics: Conference Series, 1684*(1), 12023. (2020). https://doi.org/10.1088/1742-6596/1684/1/012023
23. Nandakumar, K., Jain, A. K. & Nagar, A. Biometric template security. *EURASIP J. Adv. Signal Process.* **2008** (1), 579416. https://doi.org/10.1155/2008/579416 (2008).
24. Sundararajan, K. & Woodard, D. L. Deep learning for biometrics: a survey. *ACM Comput. Surveys*. **51** (3), 1–34. https://doi.org/10.1145/3190618 (2019).
25. Singh, M., Singh, R. & Ross, A. A comprehensive overview of biometric fusion. *Inform. Fusion*. **52**, 187–205. https://doi.org/10.1016/j.inffus.2018.12.003 (2019).
26. Shilina, S. Biometrics in online media: an anti-crisis paradigm shift. Vestnik Rossiĭskogo Universiteta Druzhby Narodov Seriîà Literaturovedenie Zhurnalistika. **28** (4), 741–748. https://doi.org/10.22363/2312-9220-2023-28-4-741-748 (2023).
27. Sultana, M., Paul, P. P. & Gavrilova, M. in *International Conference on Cyberworlds* 271–278 (IEEE, 2014). (2014).
28. Tumpa, S. N. et al. *In Advancements in Computer Vision Applications in Intelligent Systems and Multimedia Technologies*1–24 (IGI Global, 2020).
29. Alsaadi, I. M. Study on most popular behavioral biometrics, advantages, disadvantages and recent applications: a review. *Int. J. Sci. Technol. Res.* **10** (2021).
30. Wang, W. Criminal Law Regulation of Biometric Information's dissemination risk: a content analysis based on 525 Criminal Judgment documents. *Journalism Communication*. **07**, 75–88 (2022).
31. Lin, L. Construction of Associated privacy protection mechanism for biometric identification. *Youth Journal.* **5**, 34–38 (2022).
32. Cheng, S. Research on ethical issues in the dissemination of Biometric Information. *China Publishing J.* **1**, 34–38 (2023).
33. Gao, Y. Hierarchical rules for the Protection of Biometric Information. *Contemp. Communication.* **1**, 87–91 (2023).
34. Lin, A. & Lin, Q. The Technical Risks and ultiple regulation of AI face swap. *Future Communication*. **1**, 60–69 (2023).
35. Zhang, X. & Wang, X. Research on the risks and governance of facial recognition technology and its application. *Stud. Sci. Sci.* **3**, 385–393 (2023).
36. Lancelot Miltgen, C., Popovič, A. & Oliveira, T. Determinants of end-user acceptance of biometrics: integrating the big 3 of technology acceptance with privacy context. *Decis. Support Syst.* **56** (1), 103–114. https://doi.org/10.1016/j.dss.2013.05.010 (2013).
37. Lehto, X. Y., Park, S., Mohamed, M. E. & Lehto, M. R. Traveler attitudes toward biometric data-enabled hotel services: can risk education play a role? *Cornell Hospitality Q.* **64** (1), 74–94. https://doi.org/10.1177/19389655211063204 (2023).
38. Hong, Y. Preliminary Exploration of the Legal Regulation of Facial Recognition Technology. *China Inform. Secur.* **8**, 85–87 (2019).
39. Zeng, X., Liang, Z. & Zhang, H. Regulatory path of the European Union's Artificial Intelligence and its Enlightenment to China: an analysis of the Artificial Intelligence Act. *Electron. Government*. **9**, 63–72 (2022).
40. Daily, S. M. *Two years of the Data Security Law: Over half of respondents feel increased security, but concerns about rights protection persist*, (2023). https://m.mp.oeeee.com/a/BAAFRD000020230831841818.html
41. Sørensen, M. & Christiansen, A. *Ulrich Beck: An Introduction to the Theory of Second Modernity and the risk Society* (Routledge, 2012).
42. Zhang, T. The dilemma of personal information identification standards and its solution: an explanatory path based on risk society theory. *Stud. Socialism Chin. Characteristics*. **3**, 106–114 (2023).
43. Newland, J. & Furnham, A. Perceived availability of social support. *Pers. Indiv. Differ.* **27** (4), 659–663 (1999).
44. Zhou, T. Examining the critical success factors of mobile website adoption. *Online Inf. Rev.* **35** (4), 636–652 (2011).
45. Sarkar, U. et al. The literacy divide: health literacy and the use of an internet-based patient portal in an integrated health system—results from the diabetes study of Northern California (DISTANCE). *J. Health Communication*. **15** (S2), 183–196 (2010).
46. Lee, Y. C. The role of perceived resources in online learning adoption. *Comput. Educ.* **50** (4), 1423–1438 (2008).
47. McKnight, D. H., Choudhury, V. & Kacmar, C. Developing and validating trust measures for e-commerce: an integrative typology. *Inform. Syst. Res.* **13** (3), 334–359 (2002).
48. Bhattacherjee, A. & Sanford, C. Influence processes for information technology acceptance: an elaboration likelihood model. *MIS Q.*, 805–825. (2006).
49. Model, A. I. Trust and Tam in online shopping: an integrated model1. *MIS Q.* **27** (1), 51–90 (2003).
50. Pavlou, P. A. Consumer acceptance of electronic commerce: integrating trust and risk with the technology acceptance model. *Int. J. Electron. Commer.* **7** (3), 101–134 (2003).
51. McGrady, E., Conger, S., Blanke, S. & Landry, B. J. Emerging technologies in healthcare: navigating risks, evaluating rewards. *J. Healthc. Manag.* **55** (5), 353–365 (2010).
52. Rashid, T. & Asghar, H. M. Technology use, self-directed learning, student engagement and academic performance: examining the interrelations. *Comput. Hum. Behav.* **63**, 604–612 (2016).
53. Frewer, L. J., Howard, C. & Shepherd, R. Understanding public attitudes to technology. *J. Risk Res.* **1** (3), 221–235 (1998).
54. Rogers, E. M., Singhal, A. & Quinlan, M. M. Diffusion of innovations. In An Integrated Approach to Communication Theory and Research (432–448). Routledge. (2014).
55. Nielsen, S. B. There is new technology here that can perform miracles the discursive psychology of technological optimism in climate change policy debates. *J. Lang. Politics*. **22** (6), 826–845 (2023).
56. Johnson, S. & Acemoglu, D. *Power and Progress: Our thousand-year Struggle over Technology and Prosperity* (Hachette UK, 2023).
57. Asveld, L. & Roeser, S. (eds) *The Ethics of Technological risk* (Earthscan, 2009).
58. Sadek, M., Calvo, R. A. & Mougenot, C. Designing value-sensitive AI: a critical review and recommendations for socio-technical design processes. *AI Ethics*, 1–19. (2023).
59. Park, S. Y. An analysis of the technology acceptance model in understanding university students' behavioral intention to use e-learning. *J. Educational Technol. Soc.* **12** (3), 150–162 (2009).
60. Li, L., Mu, X., Li, S. & Peng, H. A review of face recognition technology. *IEEE Access.* **8**, 139110–139120 (2020).
61. Maltoni, D., Maio, D., Jain, A. K. & Prabhakar, S. *Handbook of Fingerprint Recognition* Vol. 2 (Springer, 2009).
62. Amrouni, N., Benzaoui, A. & Zeroual, A. Palmprint Recognition: extensive exploration of databases, methodologies, comparative assessment, and future directions. *Appl. Sci.* **14** (1), 153 (2023).
63. Malgheet, J. R., Manshor, N. B. & Affendey, L. S. Iris recognition development techniques: a comprehensive review. *Complexity* **2021**(1), 6641247 (2021).

64. Altwaijry, N. & Al-Turaiki, I. Arabic handwriting recognition system using convolutional neural network. *Neural Comput. Appl.* **33** (7), 2249–2261 (2021).
65. Kiran, P., Parameshachari, B. D., Yashwanth, J. & Bharath, K. N. Offline signature recognition using image processing techniques and back propagation neuron network system. *SN Comput. Sci.* **2** (3), 196 (2021).
66. Chandolikar, N., Joshi, C., Roy, P., Gawas, A. & Vishwakarma, M. Voice recognition: A comprehensive survey. In *2022 international mobile and embedded technology conference (MECON)* (pp. 45–51). IEEE. (2022), March.
67. He, W., Zhang, C. & Ren, L. Chinese civic scientific literacy and their attitudes toward science and technology—main findings from the 2020 national survey of civic scientific literacy in China. *Stud. Sci. Popularization*. **2**, 5–17 (2021).
68. Huang, J., Qiu, H. & Bai, J. Awareness, acceptance and willingness to buy genetically modified foods in urban China. *China Soft Sci.* **2**, 61–67 (2006).
69. China, C. A. o. *Notice of the Cyberspace Administration on soliciting public opinions on the Regulations on the Safety Management of the Application of Facial Recognition Technology (Trial) (Draft for Comments)*, (2023). http://www.cac.gov.cn/2023-08/08/c_1693064670537413.htm
70. Cho, J. H., Chan, K. & Adali, S. A survey on trust modeling. *ACM Comput. Surv. (CSUR)*. **48** (2), 1–40 (2015).
71. Fornell, C. & Larcker, D. F. Evaluating structural equation models with unobservable variables and measurement error. *J. Mark. Res.* **18** (1), 39–50 (1981).
72. Ho, Y. S, Bodoff, D. & University of Haifa. The effects of web personalization on user attitude and behavior: an integration of the elaboration likelihood model and consumer search theory. *MIS Q.* **38** (2), 497–A10. https://doi.org/10.25300/MISQ/2014/38.2.08 (2014).
73. Stergiou, C., Psannis, K. E., Gupta, B. B. & Ishibashi, Y. Security, privacy & efficiency of sustainable cloud computing for big data *IoT Sustainable Comput. Inf. Syst.*, **19**, 174–184. https://doi.org/10.1016/j.suscom.2018.06.003 (2018).
74. *ValidSoft UK Limited: Rise of AI-driven Biometric Fraud: Defending Identities with Advanced Security Measures*. News Bites Pty Ltd. (2024).
75. Ladley, J. *Data Governance: How to Design, Deploy and Sustain an Effective data Governance Program* 1st edn (Elsevier Science & Technology, 2012). https://doi.org/10.1016/C2011-0-04633-1
76. Koo, Y. H. Power Relationship of Gaze in the modern society through the super-panopticon as multi-networks supervision. *J. Korea Contents Association*. **9** (10), 102–109 (2009).
77. Manders-Huits, N. Regulating invisible harms. In Innovating Government: Normative, Policy and Technological Dimensions of Modern Government (57–73). The Hague, The Netherlands: TMC Asser. (2011).
78. Krisnaningsih, E., Dwiyatno, S., Jubaedi, A. D. & Shafitri, A. Increasing ethical understanding of the Use of Information Technology through Digital Literacy Proficiency Training. *Dinamisia: Jurnal Pengabdian Kepada Masyarakat*. **7** (3), 789–801 (2023).
79. Mangalaraj, G., Singh, A. & Taneja, A. IT Governance Frameworks and COBIT-A Literature Review. In *AMCIS*. (2014), August.
80. Law, J. On sociology and STS. *Sociol. Rev.* **56** (4), 623–649 (2008).
81. Maharani, E. The fourth estate unbound: examining press law and ethics in the digital age in Indonesia. *Indonesia Media Law Rev.* **3** (1). https://doi.org/10.15294/imrev.v3i1.78901 (2024).

Acknowledgements

This article acknowledges the insightful suggestions and efforts peer reviewers contribute.

Author contributions

W.Z. designed the framework of the article and research models, analyzed data, and wrote the draft of article. H.Z. proofread, polished, and implemented the article. Z.D.: data analysis, review and editing.

Funding

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Declarations

Competing interests

The authors declare no competing interests.

Additional information

Correspondence and requests for materials should be addressed to H.Z.

Reprints and permissions information is available at www.nature.com/reprints.

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.