総務省 学術雑誌『情報通信政策研究』 第８巻第２号
Journal of Information and Communications Policy Vol.8 No.2

調査研究ノート（査読付）

Facial Recognition and Personal Autonomy: Ethical Dilemmas of Surveillance in the AI age

Zhang Kaihui[1]

Abstract

In recent years, facial recognition technology has become a prominent form of artificial intelligence (AI) technology, significantly impacting society. Although this technology offers various benefits, its application faces numerous ethical criticisms. While previous studies have focused on privacy concerns related to facial recognition technology, this study argues that these technical challenges and privacy issues are deeply connected to the broader ethical problem of autonomy, and explores the specific impact of facial recognition technology on individual autonomy. This study argues that facial recognition technology affects personal autonomy in two major ways. Algorithmic bias and data manipulation interfere with personal judgment, undermining autonomy by influencing decision-making processes. Additionally, the erosion of intellectual privacy restricts the freedom to think and explore ideas without external oversight, further weakening individual autonomy. Section 2 explores autonomy as a crucial ethical value in the age of artificial intelligence. Section 3 identifies the specific risks that facial recognition technology poses to individual autonomy. Finally, Section 4 discusses the necessary considerations for balancing the benefits of facial recognition technology with its ethical risks. This approach reevaluates the concept of autonomy in the age of AI and adds new depth to ethical and social discussions thereof.

Keywords: Surveillance, Artificial Intelligence, Facial Recognition, Privacy, Autonomy

１．Introduction

The structure of a human face is unique to each individual, making it one of the most familiar biometric features. Facial recognition technology leverages the uniqueness of personal identification to play a significant role in public safety through identity verification and access control. With the introduction of deep learning methods, the accuracy of recognition and adaptability to various environmental factors have improved, broadening the applications of facial recognition technology (Adjabi et al. 2020). In China, facial recognition technology has been extensively deployed by public safety agencies, as exemplified by the arrest in 2018 of an economic crime suspect at a concert with 50,000 attendees using real-time facial recognition systems ("Chinese Man Caught by Facial

[1] Zhang Kaihui(張 開慧),a third-year doctoral student at the Graduate School of Humanities and Social Sciences, Hiroshima University

Recognition" 2018). Technology also plays a crucial role in fields such as entertainment and smart healthcare (Rawal and Stock-Homburg 2022, Dhuheir et al. 2021), facilitating natural and socially accepted human-robot interactions and the early detection of depression and stress by identifying patient emotions. Unlike other data collection methods, facial images can be obtained quickly without physical contact, thereby enhancing data collection efficiency (Adjabi et al. 2020).

However, while offering these conveniences, facial recognition technology faces numerous challenges, including ethical issues related to privacy. The widespread adoption of facial recognition technology increases the likelihood of individuals' facial images being monitored, tracked, and used without explicit consent, thereby raising societal concerns about privacy protection.

While previous studies have focused on privacy concerns related to facial recognition technology, this study argues that these technical challenges and privacy issues are deeply connected to the broader ethical problem of autonomy, and explores the specific impact of facial recognition technology on individual autonomy.

This study explores the impact of facial recognition technology on individual autonomy, combining theoretical analysis with case studies at both corporate and national levels. By leveraging data manipulation and algorithmic biases, facial recognition technology interferes with decision-making processes, undermining autonomous judgment and independent choices. Moreover, through violations of intellectual privacy, it limits freedom of thought and expression, further hindering the development of critical thinking and the capacity for independent reflection.

２．The Significance and Importance of Autonomy in the Age of Artificial Intelligence

Autonomy refers to the capacity to make decisions independently. According to Christman, individual autonomy entails leading one's life based on personal reasons and motivations, free from external manipulation or distortion (Christman 2020). Similarly, Ryan and Deci define autonomy as having its "primary etymological meaning of self-governance or rule by the self," distinguishing it from heteronomy, which involves regulation imposed by external forces (Ryan and Deci 2006).

Building on these perspectives, this study defines autonomy as "an individual's ability to make independent decisions grounded in personal reasons and intrinsic motivations." This independence encompasses freedom from external interference and the capacity for self-direction, reflecting two interrelated dimensions: the independence of behavioral choices and the self-regulation of thought.

Behavioral independence enables individuals to make decisions aligned with their values and reasoning, free from external coercion. Self-regulation of thought involves guiding cognitive and behavioral processes through intrinsic motivation, empowering individuals to freely explore, form, and express ideas. Together, these dimensions embody true self-governance and proactive agency.

It is important to acknowledge that the definition, conditions, and value of personal autonomy have been extensively debated within scholarly literature. The definitions provided in this study are not intended as an exhaustive review of this vast discourse; rather, they serve to clarify the specific perspective and analytical framework adopted here. Building on this conceptual foundation, the following section will explore the implications of autonomy in the age of Artificial Intelligence (AI), focusing on how autonomy can be redefined and practiced in a context where technological systems increasingly shape the decision-making process.

２．１．Manipulation of Decision-Making and Autonomy

With the rapid development and widespread adoption of AI technology, its influence on human decision-making has emerged as a crucial issue in academic and societal discourse. In this technology-driven era, AI has seamlessly integrated into diverse domains, including information acquisition, healthcare, education, and public services. While these advancements provide undeniable benefits, they also pose profound challenges to the independence of individual decision-making, redefining the traditional understanding of autonomy in the digital age. This study identifies two primary mechanisms through which AI disrupts decision-making independence: implicit algorithmic interventions and overt technological dependence.

AI technologies subtly shape individual decisions through algorithmic recommendation systems, whose impacts often remain unnoticed in daily life. By analyzing user behavior, these systems deliver personalized content that not only influences but may also distort individual choices under the guise of convenience. For instance, targeted internet advertisements have been shown to activate users' reward systems, encouraging impulsive consumption that can lead to financial burdens or dependency (Bault and Rusconi 2019). Similarly, the "information cocoon" effect in news recommendations restricts users' exposure to diverse perspectives (Peng and Liu 2021), while social media amplifies this by spreading political misinformation, reinforcing preexisting biases and exacerbating societal polarization. (Garrett 2019). Such algorithm-driven interventions may have far-reaching implications, fundamentally reshaping long-term decision-making patterns.

Moreover, AI-driven user interface designs often employ explicit manipulative strategies, such as "dark patterns,"(Gunawan et al. 2022) which exploit cognitive and emotional biases to influence user behavior. These strategies, enhanced by AI, have evolved into "emotional dark patterns," (Alberts et al. 2024) deploying emotionally charged prompts like "Do you really want to leave? I'll be lonely" to prolong user engagement. Together, implicit algorithmic shaping and explicit manipulative designs create a dual threat, significantly undermining individual autonomy in decision-making.

Beyond algorithmic influence, the growing reliance on AI technologies across various domains has given rise to a phenomenon of technological dependence. In healthcare, for

example, AI diagnostic tools provide treatment recommendations for physical and mental health conditions, often earning higher levels of trust and engagement from patients compared to human doctors (Dhuheir et al. 2021, Zaman et al. 2022, Habicht et al. 2024). While this trust can enhance treatment outcomes, it also raises concerns about diminished critical thinking and reduced patient autonomy, as individuals may forego seeking second opinions or fail to fully understand the rationale behind AI-generated recommendations, potentially resulting in negative outcomes such as psychological dependency (Fiske et al. 2019).

Similarly, with the rise of generative AI, individuals increasingly rely on AI for academic writing, problem-solving, and even personal life planning (Bozkurt et al. 2023, Boussioux et al. 2024). Although this reliance boosts efficiency, it risks shifting individuals from active engagement to passive dependence, ultimately weakening independent thinking and problem-solving capacities. Some studies suggest that while generative AI can enhance mathematical problem-solving skills and critical thinking (Barana et al. 2023), over-reliance on AI may simultaneously weaken individuals' capacity for critical exploration and autonomous learning (Zhai et al. 2024)

From the covert influence of algorithmic systems to the overt challenges posed by technological dependence, AI technologies are fundamentally altering individuals' ability to make independent decisions.

２．２．Safeguarding Self-Regulation of Thought

On the one hand, the self-regulation of thought represents a fundamental dimension of autonomy. It serves not only as a prerequisite for individuals to form independent judgments but also as a safeguard for sustaining intrinsic motivation and fostering critical reflection. However, the realization of this cognitive autonomy is inextricably tied to the protection of privacy. The concept of "the right to be alone," proposed by Louis Brandeis and Samuel Warren in 1890, establishes privacy as a fundamental right, emphasizing the individual's freedom from unnecessary interference (Warren & Brandeis 1890). This idea highlights the role of privacy in enabling individuals to think, explore, and act independently.

Building on the importance of privacy, Bloustein argues that its violation undermines human dignity by eroding the essential elements of freedom and individuality. He frames privacy as a cornerstone for preserving personal autonomy, as it protects the individual's capacity to maintain their unique identity and moral agency (Bloustein 1964). Meanwhile, Reiman asserted that privacy is essential for establishing ownership over one's physical and mental existence. He emphasizes that this ownership transcends mere consciousness and encompasses a moral dimension rooted in societal recognition and respect for personal boundaries (Reiman 1976). Similarly, Kupfer extends this discussion by linking privacy directly to autonomy, arguing that it fosters a coherent self-concept. He asserts that autonomy depends on individuals perceiving themselves as empowered

to shape their lives—a perception that privacy plays a crucial role in sustaining (Kupfer 1987).

While these scholars approach privacy from different perspectives—dignity, identity, and autonomy—they collectively underscore its vital role in supporting the freedom to think, act, and govern oneself independently. Privacy serves as a necessary condition for maintaining individuality and self-determination in both personal and societal contexts.

In the age of AI, the concept of intellectual privacy extends traditional notions of privacy by emphasizing the individual's ability to think, explore, and express ideas independently. As Richards argues, intellectual privacy is critical for safeguarding individuals from the chilling effects of surveillance and manipulation, both of which threaten authentic and independent thinking (Richards 2013).

Building on this analysis, the following section will further explore how technological systems, particularly in the context of surveillance and algorithmic manipulation, constrain freedom of thought and challenge the very foundations of intellectual privacy.

Based on the preceding discussion, it is evident that the age of AI profoundly challenges traditional conceptions of autonomy. As previously defined—"the ability of an individual to make decisions independently based on personal reasons and motivations"—autonomy must now be reinterpreted in the context of deep technological integration. Specifically, in the AI age, autonomy should be understood as the capacity to exercise take initiative in AI-human collaboration, engage in critical reflection and value judgment, and ensure the continuous self-regulation of thought as a safeguard against technological encroachment.

3. Potential Impacts of Facial Recognition Technology on Autonomy

Facial recognition technology identifies and authenticates individuals using facial image data (Dhuheir et al. 2021). These systems detect a face in an image, identify its location, extract facial feature vectors, and distinguish individual faces. Additionally, this technology can be used to combine facial data with other personal information for further analysis (Georgiadou et al. 2019). When combined with temporal and location information, the collected facial data enable a detailed analysis of individuals' lifestyles and behavioral patterns. Moreover, integrating facial data with social media allows a deeper understanding of personal interests, social connections, and relationships.

3. 1. Use of Facial Recognition Technology by Companies and Social Responses

Companies have faced significant criticism regarding the use of facial recognition technology. Surveillance cameras are commonly installed in shopping malls. However, such systems can lead to privacy invasion by collecting and analyzing customers' facial data without their consent. In one case, a Chinese zoo faced a significant backlash after forcing visitors to provide facial data (Allen 2019). Although the zoo claimed that it was used for security purposes, the intrusive nature of its data collection and use has drawn

widespread criticism. However, companies often analyze data they have collected to make personalized recommendations. For example, Kohler Co., an American plumbing product company, used facial recognition cameras to track store visits and utilized these data for marketing strategies and store layout optimization (Brown et al. 2021).

For online platforms, data collection exacerbates privacy issues. Social media user has increased with the proliferation of smartphones and high-speed wireless networks (Salehan and Negahban 2013). While facial data are widely shared by customers on platforms, this does not imply that companies can freely use these data. Platforms such as Facebook employ facial recognition technology for tagging and friend recommendations, which have been criticized for their privacy invasion (Damen and Zannone 2014). Although many companies obtain user consent for data collection and use through opt-out mechanisms (Burkhardt et al. 2023), privacy policies are often complex and unclear, leading users to agree without fully understanding the implications of doing so (Acquisti and Grossklags 2005).

Analyzing personal information using facial recognition technology can improve advertising effectiveness and customer satisfaction while influencing autonomous decision-making. Richards terms this behavior “persuasion” (Richards 2013) a more subtle and often more effective exercise of the power differential that can be used for blackmail. By analyzing consumer behavior, frequently displayed targeted advertisements can change consumer purchasing decisions. Such advertisements are viewed as persuasive and influential, thereby controlling individual choices and behaviors.

As profiling and analysis become more prevalent, modern marketing techniques aim to influence consumer’s decision-making. Facial recognition technology can improve the efficiency of existing market practices, making it a research subject in the marketing domain (Huang and Rust 2021). Whether this method is welcome varies among individuals. Some argue that profiling enhances the user experience by providing recommendations that align with their interests and needs.

However, if algorithms are opaque and biased, “persuasion” could lead to decisions contrary to users’ best interests. A notable example is Target (Duhigg 2012, Richards 2013), a retailer in the U.S. that identified pregnant women by analyzing customer purchase histories and sending them relevant product coupons. However, this was condemned as a privacy invasion. Target’s “pregnancy prediction” model identified specific products that pregnant women typically buy at different stages of their pregnancy, such as unscented lotions, vitamins, and cotton balls. Using this model, Target sent personalized coupons for baby products to customers who were likely to be pregnant even if they had not explicitly disclosed that information. In one notable incident, a father protested to Target after his teenage daughter received pregnancy-related coupons. He later discovered that his daughter was pregnant, which caused distress within his family, highlighting the ethical and privacy concerns of such

predictive analytics.

Furthermore, algorithms can shape user behavior and preferences over time, potentially diminishing autonomous decision-making. Turkle has emphasized how digital interfaces and algorithm-driven platforms can subtly influence thoughts, emotions, and decisions by providing information based on past behaviors, prioritizing similar opinions, narrowing perspectives, and predicting future actions (Turkle 1997). Through observations and interviews, she explored how children and older adults interact with social robots, digital pets, and other smart devices, finding that such interactions can alter children's understanding of emotional relationships and lead to emotional dependencies in older adults. Turkle's insights suggest that our cognitive landscapes are molded by the algorithmic environments we engage with daily. This shaping of thought and perception raises significant ethical concerns about the autonomy and diversity of human experience. Therefore, the critical examination and regulation of these technologies, including facial recognition, are essential.

Therefore, algorithmic "persuasion" effects are not always beneficial, as some proponents claim. Misuse or abuse can harm individuals and severely affect personal interests. Moreover, this "persuasion" continues to shape our thinking, and such shaping is not always in our best interest.

3．2．National Surveillance and Intellectual Privacy

The discussion changes when the government, rather than private companies, is the primary entity conducting surveillance. For instance, China's "Skynet" system combines millions of surveillance cameras with facial recognition technology for extensive monitoring to ensure public safety and track criminals ("Facial Recognition, AI and Big Data" 2017). The UK is one of the most surveillance countries, with a vast network of public and private surveillance cameras, and government authorities monitoring Internet traffic (Richards 2013). Although security is often cited to justify privacy invasions, the legitimacy of surveillance remains debatable (Hirschprung et al. 2022), with persistent concerns regarding privacy violations and the surveillance society.

Richards introduced the concept of "intellectual privacy," emphasizing that the greatest harm to government surveillance is its impact on the freedom to develop new ideas away from public scrutiny. He argued that such privacy is crucial for intellectuals to maintain a free society by supporting the fundamental civil liberties of thought and belief formation without interference (Richards 2013). Using Jeremy Bentham's concept of Panopticon (Bentham 1995), Richards illustrated how surveillance might alter individuals' behavior, leading to self-censorship and limited autonomy as they avoid expressing or exploring controversial ideas to evade negative surveillance outcomes. He contends that a truly free society must protect the right to private thinking, consultation, and broader social rights, such as associations, to encourage intellectual diversity and individual uniqueness.

Richards also addresses whether freedom is limited even if individuals are unaware of surveillance (Richards 2013). Extensive surveillance programs are unlikely to maintain confidentiality, and just as power disparities exist between companies and consumers, significant power disparities exist between governments and citizens, with government "persuasion" remaining strong. Surveillance thus also affects individual freedom and autonomy.

３．３．Cultural Acceptance of Surveillance and Individual Freedom

Richards compellingly argues that large-scale surveillance poses significant threats to democracy by undermining both freedom of thought and individual autonomy. Drawing on Bentham's concept of the Panopticon, he demonstrates how modern surveillance technologies foster a condition of perpetual visibility. However, Foucault in *Discipline and Punish* (Foucault 1975), extends the Panopticon beyond Bentham's architectural model, framing it as a metaphor for modern power structures. While Richards highlights the implications of surveillance for autonomy, Foucault focuses on its role in societal control. He argues that visibility compels individuals to internalize authority, aligning their actions with disciplinary norms even in the absence of direct observation. This process of self-discipline, driven by the uncertainty of being watched, makes surveillance enduring and deeply embedded, shaping not only behavior but also individuals' self-perception.

As previously noted, surveillance has shifted from passive observation to predictive and manipulative control, with algorithmic systems not only monitoring but actively shaping individual preferences and decisions. Mechanisms like personalized recommendations and information filtering reinforce existing beliefs and behaviors, leading to the "information cocoon" effect.

Complementing Foucault's Panopticon, Mathiesen's concept of the Synopticon provides a contrasting perspective by emphasizing the role of mass media and collective surveillance (Mathiesen 1997). While the Panopticon describes a system in which the few observe the many, the Synopticon illustrates how the many observe the few through mass media and technological platforms. This creates an illusion of democratized surveillance, where the public appears to hold those in power accountable. However, Mathiesen exposes a more insidious reality: powerful actors strategically engineer and manipulate information flows to control public discourse. This subtle form of control shapes the thoughts and behaviors of the majority, creating an illusion of autonomy where individuals believe they are acting independently, even as their choices are subtly directed.

Integrating Richards' Panopticon analysis, Foucault's theoretical expansion, and Mathiesen's Synopticon, modern surveillance society reveals a multi-layered and bidirectional power structure. Individuals face constant observation and ideological influence, where algorithms, personalized recommendations, and biased information

flows erode critical thinking and self-regulation. Surveillance extends beyond disciplining behavior, penetrating cognition to shape how individuals think, judge, and act. As a result, autonomy—both in behavior and thought—is fundamentally undermined.

However, this study argues that the Panopticon-Synopticon framework can be critically examined from at least two perspectives. Firstly, as the Synopticon emphasizes the majority's surveillance of the minority, it highlights that modern surveillance is not purely unidirectional but increasingly bidirectional. Advances in technologies such as social media and public platforms have empowered individuals with tools to engage in reverse surveillance. For example, the public can monitor the actions of authorities, corporations, and other individuals through online platforms, thereby challenging the traditional unidirectionality of surveillance. Public scrutiny and demands for transparency can, to some extent, limit the absolute control of those in power and safeguard intellectual privacy and freedom of thought.

Nevertheless, as Mathiesen cautions, this perspective has some important limitations. While reverse surveillance creates opportunities for reflection and resistance, the inherent inequality in technological resources and the manipulation of algorithms significantly constrain its practical efficacy. Power structures retain substantial control over technological platforms, making it difficult for individuals to truly challenge the dominance of the surveillance society. Thus, although reverse surveillance may partially mitigate the erosion of intellectual privacy, the preservation of individual autonomy in the age of artificial intelligence remains a pressing challenge.

Secondly, this study argues that in modern society, security and freedom are interdependent concepts requiring a dynamic balance. While privacy and freedom of thought are central to autonomy, the realization of individual freedoms becomes untenable if security cannot be assured. In the age of AI, surveillance technologies offer tools for efficient governance, particularly in addressing global threats such as terrorism, public health crises, and cyberattacks. For instance, data tracking during epidemics has proven effective in curbing the spread of viruses such as Cocoa, a surveillance application used in Japan to prevent the spread of COVID-19, and urban surveillance systems play a critical role in maintaining law and order.

Cultural differences play a significant role in shaping societal attitudes toward the balance between security and privacy. Thompson et al.'s research comparing cultural differences in Australia and Sri Lanka revealed how cultural factors such as power distance and individualism-collectivism affect privacy concerns, trust, and acceptance of surveillance (Thompson et al. 2020). Their study found that the relationship between privacy concerns and surveillance acceptance is weaker in high-power-distance cultures such as Sri Lanka, while collectivist cultures exhibit stronger connections between privacy concerns and protection.

Similarly, Kostka's examination of public acceptance of facial recognition technology

across China, Germany, the UK, and the US revealed the highest acceptance in China and the lowest in Germany, with the UK and the US falling in between (Kostka et al. 2021). Across these countries, convenience and security were often prioritized over privacy concerns.

Heek et al.'s empirical research further suggests that the acceptance of surveillance technology depends on specific usage scenarios and locations (Heek et al. 2016). They argue that safety needs often outweigh privacy concerns in public spaces, while the reverse holds true in private settings. Additionally, perceptions of crime threats significantly influence public acceptance of surveillance technologies.

These cultural and contextual differences highlight the complexity of achieving a balance between security and freedom in the governance of surveillance technologies. They also highlight that the legitimacy and legality of such technologies depend not only on the security value they provide but also on their respect for individual rights and socio-cultural diversity. As societal priorities and cultural values vary across contexts, addressing this trade-off on a global scale requires a nuanced and context-sensitive approach. Achieving this balance is a multifaceted challenge that demands thoughtful and inclusive policy-making.

While the above discussion of facial recognition technology has examined the issue separately for private companies and governments, Snowden's revelations highlight the close cooperation between private companies and governments in utilizing information technology (Lyon 2014). This includes customer analytics, joint surveillance, and data sharing between governments and private companies. Governments use warrants and direct purchases to access data from private companies. This cooperation blurs public-private boundaries, necessitating an integrated analysis of surveillance. This cooperation strengthens the surveillance networks, making it increasingly difficult to balance security and autonomy.

According to Kupfer, privacy is closely related to trust (Kupfer 1987). Respecting individual privacy indicates trust in one's autonomy and decision-making abilities, which helps individuals develop a trustworthy self-concept. However, extensive surveillance networks resulting from government-private cooperation could trigger a social trust crisis, eroding societal trust and undermining the foundation of autonomy. The case of East Japan Railway Company (JR East) illustrates this principle (Ozaki 2022). In July 2021, JR East introduced facial recognition functionality in some surveillance cameras, but faced public criticism for insufficiently disclosing detailed operational policies, leading to a partial withdrawal of operations. Even surveillance for security purposes can face a strong public backlash, especially when complicated by government-private cooperation, as shown in this case.

Overall, surveillance systems resulting from public-private cooperation expand the scope and depth of surveillance and pose unprecedented challenges to individual autonomy. Ensuring that facial recognition technology usage respects autonomy while

maintaining security requires a deeper examination of its impact on autonomy.

4. Balancing Technological Advancement and Respect for Autonomy

Facial recognition technology can significantly affect individual autonomy, which raises a variety of concerns. However, it is crucial not to reject this technology outright but rather to maximize its potential while addressing its ethical implications. This section proposes three key points to balance technological advancement with autonomy.

4. 1. Cultural Context

As previously discussed, the impact of facial recognition technology on individual autonomy varies according to cultural context. It is essential to understand and respect social acceptance and differences in contextual norms when introducing and deploying such technologies. Helen Nissenbaum's "Privacy as Contextual Integrity" supports this approach (Nissenbaum 2004). According to Nissenbaum, privacy should be understood and protected based on the norms governing the appropriateness and flow of information in specific contexts. This emphasizes that the appropriateness of information collection, use, and sharing depends on the context, which is crucial for ensuring that technological advancements enhance, rather than undermine, autonomy.

When applying facial recognition technology, it is imperative to evaluate privacy and safety concerns unique to each cultural context. Transparency in information collection processes and adherence to contextual norms are necessary to mitigate ethical risks and maintain public trust. While Nissenbaum's framework may lack a clear heuristic model to help policymakers determine and apply appropriate norms across diverse contexts (Waldman 2018), it remains crucial for achieving a balance between technological innovation and ethical accountability.

Despite this limitation, Nissenbaum's emphasis on contextual integrity remains central to fostering public trust and protecting autonomy in societies adopting these technologies. As Richards argues that rejecting indiscriminate surveillance and subjecting surveillance systems to meaningful judicial oversight are essential for protecting privacy and autonomy (Richards 2013). Together, these principles highlight the importance of creating context-sensitive and ethically grounded frameworks to regulate the use of facial recognition technologies effectively.

4. 2. Human-Centered Control

As Lyon notes, the post-9/11 shift toward enhanced preventive security and policing has led to excessive data collection (Lyon 2014), which is increasingly being used to predict and analyze potential criminal activity. This trend is mirrored in the marketing industry, where efficiency is achieved through the extensive use of machines and algorithms. Although data processing costs have decreased, concerns persist regarding the quality of surveillance data and the analytical methods employed.

However, errors in or the misuse of algorithms can have irreparable consequences. Therefore, it is crucial to avoid the excessive use of facial recognition technology and adjust the usage and methods of specific functions such as prediction. A combination of human and machine is necessary to avoid an overreliance on algorithms. Currently, HCI research underscores the critical importance of human-centeredness. For instance, scholars have emphasized that maintaining human judgment and ethical considerations in the design and application of AI systems is essential (Shneiderman 2022, Schmidt 2022). By placing humans at the core of the decision-making process, we can ensure that technology is applied ethically, mitigating the risks associated with algorithmic bias or errors. This human-centered approach enables technology to serve the broader interests of society, rather than merely prioritizing efficiency or predictive accuracy.

４．３．National Legal Regulations

Countries have formulated distinct legal regulations to address the ethical issues associated with facial recognition technology. Examples include the European Union's General Data Protection Regulation (GDPR) and Japan's Act on the Protection of Personal Information. These regulations have been revised multiple times to keep pace with technological advances and evolving societal expectations. However, they remain insufficient to fully safeguard individual autonomy, highlighting the need for continuous improvements to address emerging challenges.

As discussed earlier, surveillance technologies—when subjected to transparency and bidirectional oversight—can mitigate their adverse effects on autonomy. Building on this, we argue that facial recognition technology requires more targeted and comprehensive regulatory measures to address its multifaceted ethical and societal implications.

While general privacy and data protection laws provide a foundational framework, some jurisdictions have introduced specific regulations for facial recognition technology, though these efforts are often incomplete. Current legal provisions typically rely on notice and choice mechanisms to protect individuals' control over their personal information, often requiring explicit consent. However, when companies or governments fail to provide adequate information or when users lack a clear understanding of technical complexities, the authenticity of such consent becomes questionable. As facial recognition technology continues to expand, enabling extensive surveillance and profiling, the absence of specific guidelines addressing privacy invasions and their implications for autonomy becomes increasingly evident. Moreover, inconsistent application and enforcement within existing legal frameworks risk facilitating unjust surveillance and misuse of data.

Beyond national regulations, it is crucial to address the international dimension of facial recognition technology. Globalization amplifies the challenges associated with its deployment, as cross-border data flows and differing regulatory standards exacerbate ethical and privacy concerns. Moving forward, strengthened international cooperation is

essential for establishing unified norms and frameworks that uphold transparency, accountability, and the protection of individual autonomy on a global scale.

Addressing these issues requires strengthening regulations, fostering international cooperation, and enhancing transparency in technological operations to afford individuals greater control over their data. Future efforts should refine legal frameworks to keep pace with technological advancements, ensure accountability, and align global standards. A human-centered approach is essential to prevent over-reliance on AI systems and prioritize societal values and individual rights. Building on Nissenbaum's conception of Privacy as Contextual Integrity(Nissenbaum 2004), further work is needed to adapt context-specific norms to safeguard autonomy across diverse settings.

These efforts provide a roadmap for responsibly integrating facial recognition technology, balancing security and freedom while upholding ethical principles and protecting individual autonomy.

5. Conclusion

This study reevaluates autonomy in the AI age, promoting richer ethical discussions of facial recognition technology. It analyzes how facial authentication technology impacts autonomy by hindering self-determined judgment and weakening freedom of thought and critical thinking. Specifically, it partially clarifies how technology affects individual autonomy through the examples of large-scale national surveillance systems and of data collection and use by private companies.

While AI technology, including facial recognition, does not negatively impact individual autonomy, future advancements and legal regulations are anticipated. New approaches in research and policymaking are needed to maximize the convenience of technology while respecting personal privacy and autonomy. The issues and proposals presented in this study form a foundation for balancing technological advancement and protecting autonomy and for providing sustainable solutions that safeguard individual privacy and autonomy while leveraging the benefits of facial recognition technology.

Disclosure of Interests. The authors have no conflicts of interest to disclose.

Acknowledgment. This work was supported by JST SPRING, Grant Number JPMJSP2132. The author would also like to express gratitude to the academic advisor Dr. Okamoto Shimpei for his constructive guidance and to the anonymous reviewers for their valuable comments and suggestions.

References

1. Adjab,I., Ouahabi, A., Benzaoui, A., Taleb-Ahmed, A.: Past, present and future of face recognition: A review. Electronics 9(8), 1188 (2020). doi.org/10.3390/electronics9081188.

2. BBC News. Chinese man caught by facial recognition at pop concert (2018, April 13). https://www.bbc.com/news/world-asia-china-43751276 .
3. Rawal, N., Stock-Homburg R. M.: Facial emotion expressions in human–robot interaction: A survey. International Journal of Social Robotics 14, 1583–1604 (2022). doi.org/10.1007/s12369-022-00867-0.
4. Dhuheir, M., Albaseer, A., Baccour, E., Erbad, M., Abdallah, M., Hamdi M.: Emotion recognition for healthcare surveillance systems using neural networks: A survey. In: 2021 International Wireless Communications and Mobile Computing (IWCMC), Harbin City, China, pp. 681–687. IEEE, New York (2021). doi: 10.1109/IWCMC51323.2021.9498861.
5. Christman, J.: Autonomy in moral and political philosophy. In: Zalta, E. N. (ed.) The Stanford encyclopedia of philosophy (2020). https://plato.stanford.edu/archives/fall2020/entries/autonomy-moral/.
6. Ryan, R. M., Deci, E. L.: Self-regulation and the problem of human autonomy: Does psychology need choice, self-determination, and will? Journal of Personality 74(6), 1557–1585 (2006). doi: 10.1111/j.1467-6494.2006.00420.x
7. Warren, S. D., Brandeis, L. D.: The right to privacy. Harvard Law Review 4(5), 193–220 (1890).
8. Reiman, J. H.: Privacy, intimacy, and personhood. Philosophy & Public Affairs 6(1), 26–44 (1976). http://www.jstor.org/stable/2265060.
9. Kupfer, J.: Privacy, autonomy, and self-concept. American Philosophical Quarterly 24(1), 81–89 (1987). http://www.jstor.org/stable/20014176.
10. Faqar-Uz-Zaman, S.F., Anantharajah, L., Baumartz, P., et al.: The Diagnostic Efficacy of an App-based Diagnostic Health Care Application in the Emergency Room: eRadaR-Trial. A Prospective, Double-blinded, Observational Study. Annals of Surgery 276(5), 935-942 (2022). doi: 10.1097/sla.0000000000005614
11. Habicht, J., Dina, L. M., Stylianou, M., Harper, R., Hauser, T. U., Rollwage, M.: Generative AI-Enabled Therapy Support Tool Improves Clinical Outcomes and Patient Engagement in NHS Talking Therapies. PsyArXiv (2024). doi: 10.31234/osf.io/mj46k.
12. Fiske, A., Henningsen, P., Buyx, A.: Your Robot Therapist Will See You Now: Ethical Implications of Embodied Artificial Intelligence in Psychiatry, Psychology, and Psychotherapy. J Med Internet Res 21(5), e13216 (2019). doi: 10.2196/13216.
13. Bault, N., Rusconi, E.: The art of influencing consumer choices: A reflection on recent advances in decision neuroscience. Frontiers in Psychology 10, 3009 (2019). doi: 10.3389/fpsyg.2019.03009.
14. Garrett, R. K.: Social media's contribution to political misperceptions in US Presidential elections. PLoS One 14(3), e0213500 (2019). doi: 10.1371/journal.pone.0213500.
15. Georgiadou, Y., de By, R. A., Kounadi, O.: Location privacy in the wake of the GDPR.

ISPRS International Journal of Geo-Information 8, 157 (2019). doi.org/10.3390/ijgi8030157.

16. Allen, K.: China facial recognition: Law professor sues wildlife park. BBC News (2019, November 8). https://www.bbc.com/news/world-asia-china-50324342 .
17. Brown, T. G., Statman, A., Sui, C.: Public debate on facial recognition technologies in China. MIT case studies in social and ethical responsibilities of computing (Summer 2021). Kessinger Publishing, Whitefish, MO (2021). doi.org/10.21428/2c646de5.37712c5c.
18. Salehan, M., Negahban, A.: Social networking on smartphones: When mobile phones become addictive. Computers in Human Behavior 29(6), 2632–2639 (2013). doi.org/10.1016/j.chb.2013.07.003.
19. Damen, S., Zannone, N.: Privacy implications of privacy settings and tagging in Facebook. In: Jonker, W., Petković, M. (eds.) Secure data management, pp. 121–138. Springer, Cham (2014). doi.org/10.1007/978-3-319-06811-4_16.
20. Burkhardt, G., Boy, F., Doneddu, D., et al.: Privacy behaviour: A model for online informed consent. Journal of Business Ethics 186, 237–255 (2023). doi.org/10.1007/s10551-022-05202-1.
21. Acquisti, A., Grossklags, J.: Privacy and rationality in individual decision making. IEEE Security & Privacy 3(1), 26–33 (2005). doi: 10.1109/MSP.2005.22.
22. Richards, N. M.: The dangers of surveillance. Harvard Law Review 126(7), 1934–1965 (2013). http://www.jstor.org/stable/23415062.
23. Huang, M. H., Rust, R. T.: A strategic framework for artificial intelligence in marketing. Journal of the Academy of Marketing Science 49, 30–50 (2021). doi.org/10.1007/s11747-020-00749-9.
24. Duhigg, C.: How companies learn your secrets. The New York Times Magazine, 2012. https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html .
25. Turkle, S.: Seeing through computers: Education in a culture of simulation. American Prospect (March–April), 76–82 (1997).
26. People's Daily Online: Facial recognition, AI and big data poised to boost Chinese public safety (2017, October 17). http://en.people.cn/n3/2017/1017/c90000-9280772.html .
27. Hirschprung, R. S. Tayro, S., Reznik, E.: Optimising technological literacy acquirement to protect privacy and security. Behavior & Information Technology 41(5), 922–933 (2022). doi.org/10.1080/0144929X.2020.1842907.
28. Bentham, J. (1995). Panopticon. In The Panopticon Writings. Ed. Miran Bozovic (London: Verso, 1995). p. 29-95.
29. Thompson, N., McGill, T., Bunn, A., Alexander, R.: Cultural factors and the role of privacy concerns in acceptance of government surveillance. Journal of the Association for Information Science and Technology 71(9), 1129–1142 (2020). doi.org/10.1002/asi.24372.

30. Kostka, G., Steinacker, L., Meckel, M.: Between security and convenience: Facial recognition technology in the eyes of citizens in China, Germany, the United Kingdom, and the United States. Public Understanding of Science 30(6), 671–690 (2021). doi: 10.1177/09636625211001555.
31. Heek, J., Arning, K., Ziefle, M.: The surveillance society: Which factors form public acceptance of surveillance technologies? In: Helfert, M., Klein, C., Donnellan, B., Gusikhin, O. (eds.) Smart cities, green technologies, and intelligent transport systems, pp. 170–191. Springer, Cham (2016). doi.org/10.1007/978-3-319-63712-9_10.
32. Lyon, D.: Surveillance, Snowden, and big data: Capacities, consequences, critique. Big Data & Society, 1(2) (2014). doi.org/10.1177/2053951714541861.
33. Ozaki, O.: The use of live facial recognition technology by private entities in public places: A study of recent case in Japan. In: Kreps, D., Davison, R., Komukai, T., Ishii K. (eds.) Human choice and digital by default: Autonomy vs digital determination, pp. 27–35. Springer, Cham (2022). doi.org/10.1007/978-3-031-15688-5_3.
34. Nissenbaum, H.: Symposium: Privacy as contextual integrity. Washington Law Review 79, 119 (2004). https://digitalcommons.law.uw.edu/wlr/vol79/iss1/10.
35. Waldman, A. E.: Privacy as trust: Information privacy for an information age. Cambridge University Press, Cambridge (2018).
36. Shneiderman, B.: Human-Centered Artificial Intelligence: Reliable, Safe & Trustworthy. International Journal of Human–Computer Interaction 36(6), 495–504 (2020). doi: 10.1080/10447318.2020.1741118.
37. Schmidt, A.: Interactive Human-Centered Artificial Intelligence: A Definition and Research Challenges. Proceedings of the 2020 International Conference on Advanced Visual Interfaces (AVI '20). Association for Computing Machinery, New York, NY, USA, Article 3, 1–4 (2020). doi: 10.1145/3399715.3400873.
38. Peng, H., & Liu, C.: Breaking the Information Cocoon: When Do People Actively Seek Conflicting Information. Proceedings of the Association for Information Science and Technology, 58 (2021), 801–803. doi.org/10.1002/pra2.567
39. Gunawan, J., Santos, C., & Kamara, I.: Redress for dark patterns privacy harms? A case study on consent interactions. Proceedings of the 2022 Symposium on Computer Science and Law, (2022). doi.org/10.1145/3511265.3550448
40. Alberts, L., Lyngs, U., & Van Kleek, M.: Computers as Bad Social Actors: Dark Patterns and Anti-Patterns in Interfaces that Act Socially. Proceedings of the ACM on Human-Computer Interaction, 8(CSCW1) (2024). doi.org/10.1145/3653693
41. Bozkurt, A., Junhong, X., Lambert, S., Pazurek, A., Crompton, H., Koseoglu, S., Farrow, R., Bond, M., Nerantzi, C., Honeychurch, S., Bali, M., Dron, J., Mir, K., Stewart, B., Costello, E., Mason, J., Stracke, C. M., & Romero-Hall, E. (2023). Speculative Futures on ChatGPT and Generative Artificial Intelligence (AI): A

Collective Reflection from the Educational Landscape. Asian Journal of Distance Education, 18(1) (2023). doi.org/10.5281/zenodo.7636568

42. Boussioux, L., Lane, J. N., Zhang, M., Jacimovic, V., & Lakhani, K. R.: The Crowdless Future? Generative AI and Creative Problem Solving. Harvard Business School Technology & Operations Management Working Paper No. 24-005 (2024). doi.org/10.2139/ssrn.4533642
43. Barana, A., Marchisio, M., & Roman, F.: Fostering Problem Solving and Critical Thinking in Mathematics Through Generative Artificial Intelligence. Proceedings of the 20th International Conference on Cognition and Exploratory Learning in the Digital Age (CELDA) (2023).
44. Zhai, C., Wibowo, S., & Li, L.D.: The Effects of Over-Reliance on AI Dialogue Systems on Students' Cognitive Abilities: A Systematic Review. Smart Learning Environments, 11(28) (2024). doi.org/10.1186/s40561-024-00316-7
45. Bloustein, E. J.: Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser. In F. D. Schoeman (Ed.), Philosophical Dimensions of Privacy: An Anthology (1964). Cambridge University Press.
46. Foucault, M.: Discipline and Punish: The Birth of the Prison. Pantheon Books, (1977).
47. Mathiesen, T.: The Viewer Society: Michel Foucault's `Panopticon' Revisited. Theoretical Criminology, *1*(2) (1997). doi.org/10.1177/1362480697001002003
48. Artificial Intelligence Act: MEPs adopt landmark law(2023). https://artificialintelligenceact.eu/

(Accepted 10 Jar 2025; Published Online 24 Jar 2025)