Analysis on Privacy Issues with Facial Recognition Technology

Pengyu Jiang[1,*]

[1] School of Marxism, Shanghai Jiao Tong University, Minhang, Shanghai, China
*Pengyu Jiang. Email: jiangpengyu321@sjtu.edu.cn

ABSTRACT
The implementation of face recognition technology is simple and easy to cause abuse of technology. Its contactless nature makes privacy risks more hidden. In many contexts, people lose their autonomy in facial information. Helen Nissenbaum analyzes privacy from the perspective of information transmission. Under his "contextual integrity" theory, we can more clearly understand that the reasons for the privacy problems of face recognition technology are mainly the mismatch of information attributes, the neglect of information transmission principles, and the shortcomings of the technology itself. Based on this, in order to maintain contextual integrity, we should be guided by the principle of necessity of "matching technology with context" in technology practice. So as to improve the level of technical management and user' privacy awareness, and attach importance to the technical means of privacy protection.

Keywords: *Face recognition technology, Privacy, Contextual integrity, Privacy protection technology.*

1. INTRODUCTION

The widespread application of face recognition technology has enriched people's digital lives. In such a digital era, data intelligence based on cognitive computing transforms a single person from an individual in the sense of statistical average to an object that can be analyzed separately, a change that heralds the arrival of a data parsing society[1]. Personal information is the key to the analysis of individuals, of which face information is the most recognizable, and its leakage will lead to many adverse consequences. The privacy concerns of face recognition technology have attracted great attention. The European Parliament passed a resolution in October 2021 prohibiting police from implementing large-scale facial recognition in public places or border checks. At the societal level, Facebook decided to shut down its facial recognition system in November 2021 due to collective consumer complaints. After the official implementation of the Personal Information Protection Law in China, news reports related to face recognition technology are also gradually increasing. The privacy ethics of face recognition technology has become one of the focuses of attention in the ethics of science and technology. This paper analyzes the specific presentations of privacy problems, explores the causes of the problems from the perspective of "contextual integrity", and then proposes corresponding ethical governance paths, especially from a forward-looking perspective.

2. SPECIFIC PRESENTATIONS OF PRIVACY PROBLEMS

Simply understood, face recognition technology is a technology that extracts the features of a face through a computer and authenticates against those features. Compared with other biometric identification technologies such as fingerprint recognition, iris recognition, DNA recognition, etc., the advantages of face recognition are mainly reflected in its non-contact collection without too much aggression, which is easier to be accepted by people[2]. Since Xiaoou Tang and his team released the DeepID series of algorithms in 2014, the accuracy rate of face recognition technology has been greatly improved, and then it has developed rapidly in various fields.

In specific technical practice, the privacy problems in face recognition technology are mainly manifested in three aspects. First, the misuse of facial recognition technology increases the complexity of privacy protection. Compared with other biometric technologies, the realization of face recognition technology is universal and simple, and does not need to be equipped with a special information receiver like fingerprint or pupil recognition, as long as the device has a camera function.

The advantage of this is that the cost of applying face recognition technology is low, and some devices with cameras only need to be connected to the face recognition system. However, this advantage can easily lead to the abuse of face recognition technology. In addition to the government's widespread use of facial recognition, more and more private and commercial activities are also using facial recognition everywhere. These organizations are collecting people's face information at will, but the information management capabilities of these organizations are uneven. On personal devices such as mobile phones and computers, there can be options for consent or rejection in the collection of faces, but public devices such as access control and public cameras are difficult to implement the principle of "informed consent". Most commercial face recognition does not make any notification about the form, scope, purpose and storage time of its collection when collecting face information, let alone seeking the consent of users[3]. The abuse of face recognition devices makes privacy protection need to consider the full cycle process of technology application, including the legitimacy of the technology application itself, the ethical guidance in technical practice, and the social effects produced by technology. The complexity of privacy protection is greatly increased.

Second, the privacy risks of face recognition technology are more hidden. Its contactless nature facilitates not only the public, but also privacy violations. Compared to other biometric information, it is easier and more stealthy to obtain face information. In interpersonal communication, face information as the basis for communication, in the online world often exists as a kind of public information. People have long been accustomed to sharing personal photos or videos. But once facial information is taken away from the social context, especially for victims of online violence, it transforms into an important form of privacy message that preserves the dignity of the individual. Various face-changing videos on the Internet have proven that obtaining and processing face information from the online world has become a reality. This face information may deceive the face recognition system and harm the rights and interests without the knowledge of the parties. This shows that the privacy problems caused by face recognition technology have a strong concealment, and individuals often only realize the leakage of private information after the damage has occurred, which is a major challenge for privacy protection.

Finally, face recognition technology can easily make people lose their autonomy in face information. In the digital age, deciding who can and how to handle personal information is inherently difficult. The abuse of face recognition technology and the concealment of privacy risks make it more difficult for people to control their face information. It is both privacy and not privacy, depending on the specific situation, and the individual has the power to transform the attributes of the face information. However, the use of facial recognition technology weakens this power. In public spaces, people cannot realize when and where the collection and recognition of face information occurs, and they cannot decide which type of information the face information exists as at a certain time. In some technical practices, face information that exists as privacy is treated as non-private information by technology. The abuse of face recognition technology also creates a tendency to have a single attribute of face information, that is, it exists only as non-private information. For example, in the context of sales offices, photo album classification and access control, people cannot decide whether face information is private, nor can they control the conversion of face information attributes, losing the autonomy of face information.

3. "CONTEXTUAL INTEGRITY" IN PRIVACY PROTECTION

Defining the concept of privacy has long been a conundrum. Since Samuel Warren and Louis Brandeis first discussed the right to privacy more systematically in 1890, the concept of privacy has changed with the times. The advent of information technology has made the dissemination of information a core element in the discussion of privacy. Faced with the increasing complexity of information systems and related practical activities, Helen Nissenbaum proposed a context-based understanding of privacy, arguing that the meaning of privacy varies from context to context. Context-based information norms regulate the flow of personal information in a specific context. When these norms are contravened, we experience this as a violation of privacy, here labelled as a violation of contextual integrity[4]. In the social context, face information is an important element of interpersonal communication. It is just ordinary personal information and not private information. But in some online violence, it exists as important private information. In the current data-based technology environment, public space and private space are increasingly integrated, and privacy is no longer absolutely a kind of private information. The "context-based privacy" proposed by Nissenbaum can target specific technical practices, making people more aware of how privacy violations occur. When we can clearly understand the context behind the practice, we can realize which privacy-related parameters are being undermined. In the subsequent governance, we can maintain the stability of these parameters through legal, technical, ethical and other means. These parameters are discussed in detail below.

Context-related information norms contain four key parameters: contexts, actors, attributes, and transmission principles[4]. Contexts are the backdrop for informational norms. The framework of contextual integrity postulates a multiplicity of social contexts, each with a distinctive set of rules governing information flows. Taking medical treatment as an example, in this context, the actors have patients, doctors and hospitals. The patient is the main information subject and the sender of information, the doctor and the hospital are the recipients of information. The attribute of the information is the patient's health information. The transmission principles include "doctors should ensure that patients' health information is not known to others", "hospitals should ensure the safety of patient health information storage" and so on. When such a contextual integrity is well maintained, we believe that no privacy violations arise. If the doctor asks the patient about his or her studies, the attributes of the information do not belong to the information norms of the current context. The integrity of the context is compromised, we think that this has created a privacy violation.

Under such a "contextual integrity" perspective, there are three main reasons for the privacy problems of face recognition technology. The first category is the mismatch between the information attribute and the context. The most prominent problem is the misuse of technology due to misappropriation, which includes not only the irrational use of technology, but also the forced use of technology. With the popularity of face recognition technology, some scenes such as residential areas, zoos, sales offices, etc. have begun to be equipped with face recognition. It is true that technology has solved problems such as resident certification, tourist certification, and customer certification, but the solution of the problem has created a larger privacy problem and triggered discussions from all walks of life. In these contexts, face information is not necessary, and mandatory use actually leads to a positive effect that is less than a negative effect. Taking zoos as an example, face recognition has not brought about a significant improvement in the efficiency of tourist authentication and the comfort of tourists, but has increased the privacy crisis of tourists due to the use of sensitive face information. Many contexts require only less sensitive personal information, such as mobile phone numbers, bills, etc. The forced application of face recognition technology leads to the loss of the user's right to choose, forming a technological hegemony. The mismatch between information attributes and context destroys contextual integrity and privacy violations are highly susceptible.

The abuse of face recognition technology reflects that relevant organizations lack a correct understanding of face recognition technology before making decisions, only pay attention to their own interests, and ignore the privacy value of face information of technical audiences. Not only these organizations, but also some users do not recognize the importance of face information to personal privacy. Face recognition is easily used by organizations, and most users acquiesce to its use. Because of the wrong assessment, the information attributes do not match the context itself, even if some institutional standards are established after the use of technology, it is still impossible to solve the problem from the root cause. In the face of such problems, what needs to be done is to completely eliminate the irrationality of technology, that is, to cancel the use of technology.

The second category is the neglect of the transmission principles by technology management. The use of face recognition technology in the appropriate context will still produce certain privacy and ethical problems, such as algorithmic discrimination, lack of information autonomy, and lack of informed consent. The management of technology requires the participation of governments, technology companies and users. The Personal Information Protection Law stipulates that the processing of personal information requires the consent of the individual, and the processor of personal information shall not refuse to provide products or services on the grounds that the individual does not agree to the processing of his or her personal information or withdraws his consent. In the face of such norms, although technical managers will seek the consent of users, these "notices" will either appear in an inconspicuous place or be vague. And it is still common to be unusable to experience technical services because of disagreement.

The aforementioned behaviors reflect the deliberate evasion of informed consent principles by technology managers. It is reasonable to assume that technology managers are mostly aware of these problems, but because of other factors such as economic factors, they tend to evade the corresponding transmission principles, which leads to unstable maintenance of contextual integrity. Face information has great economic value for them. To eliminate the covert use of facial information by technology companies, ways need to be found to undermine the economic value of facial information or find new monetization models. In the face of such problems, governments, technology companies and users have been gambling. How to find a balance between the three is the biggest difficulty in solving this type of problem.

The third category is the defect of face recognition technology itself. The boundaries of such issues are clearest. Face recognition requires a database to store the user's face information, the degree of security of the database is determined by technical conditions. The instability of the technology itself leads to the instability of the information recipient, which may destroy the integrity of the context. There have been cases of criminals exploiting technology vulnerabilities to obtain database information, such as Facebook's revelation in December 2018 that 68 million users' private photos were leaked due to software vulnerabilities. The impact of leaks in the database of face information on society is often enormous. On the one hand, leaks can lead to the damage to people's interests, and on the other hand, they will also reduce public trust in technology managers. The public's understanding of technological security is simple, that is, technology protects the privacy data that is closely related to individuals[5]. Technological protection can often only be achieved by new technologies. In terms of technical protection, technology developers have made various attempts. For example, privacy-enhancing technologies use secure multi-party computation during the face recognition phase to hide biometric information and verification results from the server, thus protecting face information[6]. The solution of technical problems depends on the degree of development of the technology. While there is no technology that is absolutely secure, it is possible to use facial recognition under acceptable security risks. Compared with the first two types of problems, the privacy risks caused by technical flaws are clearer.

4. GOVERNANCE PATH FOR PRIVACY PROBLEMS

In essence, the destruction of the integrity of the information context by technological practice reflects the conflict between humanistic culture and technological culture. The immense power of technology lures people to pay too much attention to instrumental rationality, ignore value rationality, and cause various privacy problems. The problem of privacy protection is how to deal with the relationship between the two cultures, the most important thing is to rebuild the relationship between value rationality and instrumental rationality. What needs to be done is to cast instrumental rationality with value rationality[7]. Only in this way can technology always exist as a means for human beings to seek a happy life.

4.1. The Principle of Necessity: Matching Technology to Context

When scholars analyze the privacy ethics of face recognition, most of the discussions are how to solve the problems arising after the application of technology, and there is less forward-looking discussion of face recognition technology. Face recognition applications still follow the new technology application idea of "first apply and then govern"[8]. However, in many contexts, the intervention of face recognition technology has broken the reasonable information transmission norms, and the application of technology itself is a problem. As can be seen from the system framework of face recognition technology, its technical purpose is to compare the input information with the database information, and then identify a specific person. Although the application of face recognition in the field of security and finance also has some problems, there are fewer ethical controversies in comparison. The reason is that the context of the use of the two is more compatible with the technical function of face recognition, and the intervention of face recognition technology will increase the stability of the context. Technical functions determine that a specific technology must have a certain scope of application. In conducting forward-looking assessments of technology applications, guided by the necessary principle of "matching technology to context", it will help to avoid the misapplication of facial recognition technology. In the field of security, the duty of the police is to find criminal suspects in the crowd, and "identity recognition" is the core of this process. The function of face recognition technology matches this context. In contrast, in the case of Hangzhou Zoo, the ticket inspection is to screen whether tourists have purchased tickets, this process mainly identifies the authenticity of the ticket. Identity recognition has appeared in the ticket purchase stage. The use of face recognition in the ticket inspection stage has caused excessive use of technology, resulting in the risk of the corresponding contextual integrity being destroyed, so that resulting in the emergence of privacy and ethical risks.

There are two processes for matching technology to context. First, technical managers can correctly understand the function of technology. It is not difficult for people to understand the functions of face recognition technology. Technology developers should accurately introduce relevant products, not only to let managers understand the powerful capabilities of technology, but also to make necessary explanations of the possible privacy risks of technology. Second, the manager can correctly understand the context, that is, what are the core factors in the context? The problem seems simple, but it is easy for managers to ignore these thoughts. For example, cameras "identify students" is a non-essential need in the classroom. The use of face recognition is necessarily related to face information. In order to achieve a non-essential need in the classroom, the introduction of face information adds unnecessary information recipients, breaks the original contextual integrity, and inevitably produces the risk of invasion of privacy. Matching technology to context may seem simple, but achieving this requires multifaceted assessments in different contexts.

4.2. Improve Technology Management and Privacy Awareness

Technology companies rely on the power of technology to dominate in technical practice. The rules for the use of technology are set by technology companies, and people only have two choices, whether to use or not to use, and sometimes have to use. People often have no right to interfere with the rules of use. Therefore, the management of technology applications should naturally be mainly the responsibility of technology companies. From the perspective of responsibility ethics, technicians have a "forward-looking moral responsibility" for the use of technology. Most companies can recognize their responsibilities, but the problem is that some people are unwilling to fulfill this moral responsibility, and responsibility only stays at the level of rational cognition, and cannot become a living responsibility practice[9]. Therefore, the solution of the problem cannot be achieved only by technology companies. Governments and users are also indispensable. Only by working together to optimize technology management can responsible practices be made possible.

First, strengthen the social responsibility of technology companies. For technology companies, laws and regulations are the bottom line for handling personal information. As the leader of technological development, in addition to pursuing economic interests and abiding by basic laws, they should also take the initiative to assume higher social responsibilities and attach equal importance to economic interests and technical services. Although economic interests are important, it is the capital of technological progress, but technical services are directly related to people's life happiness. Compared with exploiting loopholes in laws and manufacturing technology hegemony, the economic benefits of using excellent technical services are more stable. David Coss and Gurpreet Dhillon, through experimental data collation and analysis, proposed six privacy protection goals for cloud computing technology, among which "increasing trust in technology providers" and "maximizing responsibility for information management"[10] are applicable to any information technology, and face recognition technology is no exception. The lack of public awareness of technology and the frequent occurrence of information leakage incidents make users' trust in technology low. Technical managers should focus on users to reflect the information management responsibilities they bear, and only then will they improve users' trust.

Second, refine the establishment of laws and regulations. For the government, it has become particularly important to regulate technical management through laws and regulations. The Cybersecurity Law stipulates: "Network operators collecting and using personal information shall follow the principles of legality, propriety, and necessity, disclose the rules for collection and use, clearly indicate the purpose, method, and scope of information collection and use, and obtain the consent of the person being collected." Although the Cyberspace Administration of China and other departments have issued some more detailed documents such as the “Method for Determining the Illegal Collection and Use of Personal Information by Apps”, the implementation of specific operators is not comprehensive enough. Problems such as unclear user feedback channels, obscure app privacy instructions, and targeted advertising still exist. On July 28, 2021, the Supreme People's Court issued “the Provisions on Several Issues Concerning the Application of Law in the Trial of Civil Cases Involving the Use of Face Recognition Technology to Handle Personal Information”, which shows that the problem of face recognition technology is gradually being resolved. It can also be seen from the Personal Information Protection Law of the People's Republic of China that the government has stepped up meticulous regulation of the management of personal information. In October 2021, the European Parliament passed a resolution banning police from implementing large-scale facial recognition in public places or border inspections. These measures reflect countries' efforts to refine laws and regulations, no longer just to protect people's privacy through macro principles.

Third, raise public awareness of privacy risks. For users, although they cannot get involved in the development and management of technology, as an experience party, users can feedback their personal privacy considerations to technical managers, thereby helping managers optimize management. This requires further improvement of the feedback mechanism, and also requires users to have a better sense of privacy. According to the survey of the People's Think Tank, the current public's privacy awareness belongs to a medium and slightly high level. The average public privacy awareness is 58.69, with a full score of 100. Although the public attaches great importance to the privacy protection of personal life and private space, the awareness of privacy protection in public space is still relatively weak, with more than 80% of respondents believing that private information is valuable, while only 28.89% of people “take the initiative to take protective measures”[11]. The public's awareness of privacy precautions needs to be improved. From the proliferation of face recognition technology and the rarity of corresponding litigation cases, it can be seen that people still lack a correct understanding of the privacy value of face information. The public's assessment of facial recognition technology is often utilitarian. When the immediate value of technology outweighs the immediate privacy risk, people don't refuse to use it. However, the core of risk awareness is not in the present, but in the future. Privacy risk awareness is even more so. Today's pictures and videos will only reveal the privacy problems behind them when they are associated with an event in the future.

4.3. Technical Means to Strengthen Privacy Protection

In addition to technical operations, technology companies often play a role in technology development and maintenance. The more secure the privacy of the technology, the fewer privacy management problems there will be. Face recognition technology to protect privacy mainly plays a role in the face characterization stage and the face recognition stage.

In the face representation stage, a face recognition technology that uses differential privacy can perturb face information data. After this process, the face information stored in a third-party database will no longer be the original information. After data disturbance, even if the database is leaked, the criminals will only get some messy information. Through experiments, the technology can show about 70%-90% classification accuracy under the corresponding privacy standards[12]. Differential privacy technology directly reduces the sensitivity of face information in the database and greatly improves the security of user face information. Based on this technology, users do not produce new real face information when using face recognition technology, and at the same time can ensure the normal use of technology, which not only reduces the threat of face information theft, but also improves the user's trust in technical managers and plays a direct role in solving privacy problems.

In the face recognition stage, secure multi-party computing can hide biometric information and verification results from the server. This privacy-enhancing technology uses a highly optimized encryption protocol that allows information to be exchanged between multiple parties without the need to share real information. In addition, because face recognition is easy to occur without the user's knowledge, such as personal photos on social software are recognized and classified by face recognition technology, an anonymized face information technology can help users fight against face recognition algorithms, while retaining more original information so that humans can still be recognized[13]. Anonymization can intervene in the recognition results of facial recognition technology, countering the mandatory use of facial recognition technology without affecting people sharing personal photos in social networks. Regardless of the method adopted, technicians have long been concerned about the privacy issues in face recognition technology, and have explored many technical means to protect privacy. The maturity and popularity of these technologies are crucial to solving privacy problems.

5. CONCLUSION

Whether in the field of ethics or the field of law, the importance of privacy to people is self-evident. Unlike other biometric information, face information has direct recognizability. Under the influence of information technology, the privacy risk of face information is greatly increased. The misuse of facial recognition technology and unreasonable management exacerbate privacy ethical risks. People's forward-looking assessment of the application of technology is still relatively lacking. Only when the technology matches the context, the contextual integrity can be better maintained, and the technology can truly improve people's quality of life. At the same time, after the practice of technology, technology companies, governments, and users need to work together to help the technology develop for good. Moreover, the development of the technology itself is also crucial to the solution of the privacy problem. Face recognition technology brings both opportunities and challenges. In the two stages before and after technical practice, it should be regulated and guided accordingly. In the future, it is necessary to improve people's understanding of the privacy value of face information and explore new information profit models. This requires the joint efforts of humanities and technology.

AUTHORS' CONTRIBUTIONS

With the help of Helen Nissenbaum's theory of "contextual integrity", the author states the privacy problems of face recognition technology, explores the reasons behind it, and then proposes some solutions.

ACKNOWLEDGMENTS

Thanks to Helen Nissenbaum's theory of privacy, it gives the author a new way of thinking about privacy of information technology. And sincerely gratefully acknowledge the author's supervisor Professor Yanyong Du for his encouragement and support to all aspects of the author.

REFERENCES

[1] Duan Weiwen. Artificial Intelligence and the Emerging of Analytical Society. Science and Society, 2019, vol. 9, pp. 115-128. DOI: https://doi.org/10.19524/j.cnki.10-1009/g3.2019.01.115

[2] Duan Jin. Face Automatic Machine Recognition. Science Press, Beijing, 2009.

[3] Jiang Fuming, Zeng Huiping. Ethical issues relating to privacy in the application of face recognition technology and solutions. Social Science Journal of Universities in Shanxi, 2020, vol. 32, pp. 19-24. DOI: https://doi.org/10. 16396 /j. cnki . sxgxskxb. 2020. 09. 005

[4] H. Nissenbaum. Privacy in context: Technology, Policy, and the Integrity of Social Life. Stanford University Press, Stanford, California, 2010.

[5] Yang Qingfeng. (2018) Data sharing and privacy protection: philosophical demonstration on the technological scheme. Studies in Dialectics of Nature, 2018, vol. 34, pp. 111-116. DOI: https://doi.org/10.19484/j.cnki.1000-8934.2018.05.018

[6] Z. Erkin, M. Franz, J. Guajardo, et al. Privacy-Preserving Face Recognition, in: Goldberg I, Atallah M. (Eds.), Privacy Enhancing Technologies. Springer, Heidelberg, 2009, pp. 235-253. DOI: https://doi.org/10.1007/978-3-642-03168-7_14

[7] Wang Jinzhu. Review on the “difficulty” of privacy. Studies in Dialectics of Nature, 2020, vol. 36, pp. 68-73. DOI: https://doi.org/10.19484/j.cnki.1000-8934.2020.06.013

[8] Duan Weiwen. Face recognition: "Naked running" era of us. Business Management Review, 2021, pp. 119-120.

[9] Long Jingyun. New responsibility ethics: an important guarantee for a better life in the era of technology. Journal of Central China Normal University(Humanities and Social Science), 2021, vol. 60, pp. 90-100.

[10] D. Coss, G. Dhillon. Cloud privacy objectives a value based approach. Information & Computer Security, 2019, vol. 27, pp. 189-220. DOI: https://doi.org/10.1108/ICS-05-2017-0034

[11] Zhang Jie. The current survey report on the public's information security awareness and privacy concept. Governance, 2020, pp. 44-48. DOI: https://doi.org/10.16619/j.cnki.cn10-1264/d.2020.14.010

[12] M. Chamikara, P. Bertok, I. Khalil, et al. Privacy Preserving Face Recognition Utilizing Differential Privacy. Computers & Security, 2020, vol. 97, pp. 1-12. DOI: https://doi.org/10.1016/j.cose.2020.101951

[13] B. Driessen, M. Dürmuth. Achieving Anonymity against Major Face Recognition Algorithms, in: Decker B, Dittmann J, Kraetzer C, et al. (Eds.), Communications and Multimedia Security. Springer, Magdeburg, 2021, pp. 18-33. DOI: https://doi.org/10.1007/978-3-642-40779-6_2