Acta Bioethica 2022; 29(1): 259-268. http://dx.doi.org/10.4067/S1726-569X2023000200259

FACE, FACIAL RECOGNITION TECHNOLOGY AND PERSONAL PRIVACY

Wei Li[1], Menglian Hua[2], Ying Sun[3], Husheng Li[4], Yanhu Lin[5*]

Abstract: The privacy problem of facial recognition technology is that commercial companies obtain people's facial information without the consent of individuals and use facial information to infringe on the privacy of individuals. The importance of human privacy in facial recognition technology is reflected through facial ethics, which requires others to perform corresponding obligations to individuals, such as oral care. Through the analysis of the privacy issues of facial recognition technology, it is found that the two elements of "without personal informed" and "without personal consent" together form the basis for commercial companies to violate personal privacy. The principle of informed consent includes the principle of informed and the principle of consent, which is derived from the principle of informed consent in medical ethics. This paper improves the principles of informed consent in medicine and ethics to better address facial recognition privacy issues.

Keywords: facial recognition technology; privacy issues; facial ethics; informed consent

Rostro, tecnología de reconocimiento facial y privacidad personal

Resumen: El problema de la privacidad en la tecnología de reconocimiento facial es que las empresas comerciales obtienen información facial de las personas sin el consentimiento de éstas y utilizan la información facial para vulnerar la privacidad de las personas. La importancia de la privacidad de las personas en la tecnología de reconocimiento facial se refleja a través de la ética facial, que exige que otros cumplan las obligaciones correspondientes con los individuos, como el cuidado bucal. A través del análisis de los problemas de privacidad de la tecnología de reconocimiento facial se descubre que los dos elementos de "sin información personal" y "sin consentimiento personal" juntos forman la base para que las empresas comerciales violen la privacidad personal. El principio de consentimiento informado incluye el de información y el de consentimiento, que se deriva del principio de consentimiento informado de la ética médica. Este artículo mejora los principios del consentimiento informado en medicina y ética para abordar mejor los problemas de privacidad del reconocimiento facial.

Palabras clave: tecnología de reconocimiento facial; cuestiones de privacidad; ética facial; consentimiento informado

Face, tecnologia de reconhecimento facial e privacidade pessoal

Resumo: A questão da privacidade na tecnologia de reconhecimento facial é que as companhias comerciais obtém informações faciais das pessoas sem seu consentimento e usam informação facial para infringir sua privacidade. A importância da privacidade humana na tecnologia de reconhecimento facial é refletida através da ética facial, que exige que se cumpram obrigações correspondentes para com os indivíduos, da mesma forma como com cuidados orais. Através da análise de aspectos de privacidade na tecnologia de reconhecimento facial, encontrou-se que os dois elementos "sem informação pessoal" e "sem consentimento pessoal" juntos, formam a base para companhias comerciais violarem a privacidade pessoal. O princípio do consentimento informado inclui o princípio de informação e o princípio de consentimento, os quais derivam do princípio do consentimento informado em ética médica. Esse artigo melhora os princípios do consentimento informado em medicina e ética para melhor incluir aspectos de privacidade no reconhecimento facial.

Palavras chave: tecnologia de reconhecimento facial; aspectos de privacidade; ética facial; consentimento informado

[1] School of History and Culture of Science, School of Marxism, Shanghai Jiao Tong University, Shanghai 200240, China

[2] School of Marxism, Shanghai University of Finance and Economics, Shanghai 200433, China

[3] School of Humanities, Shanghai University of Finance and Economics, Shanghai 200433, China

[4] School of Public Health, Fujian Medical University, Fuzhou 350122, China

[5] School of Marxism, Chengdu University of Traditional Chinese Medicine, Chengdu 611137, China,
Corresponding author: linyanhu12@163.com

1. Introduction

There is a huge market demand for facial recognition technology due to its convenience and security. In the future, with the improvement of accuracy and speed of facial recognition technology, it will be widely accepted around the world. The gradual popularization and application of facial recognition technology in society have made people feel the safety and convenience of facial recognition. But do people think about the technology and the various rights violations it causes when using facial recognition technology? It is undeniable that the emergence of facial recognition technology can indeed bring people convenience and safety, but is convenience and safety really what users want? When users' rights, especially privacy rights, are violated, What should users do?

Commercial companies in the real world use facial recognition technology to develop products to meet people's needs on the one hand and use facial recognition technology to obtain facial information of users or individuals for other purposes, such as better price discrimination. In the process of people using facial recognition technology, people's privacy rights are constantly being taken away. Faced with the privacy problems of facial recognition technology, this paper believes that the principle of informed consent in medical ethics can effectively solve the above problems.

This paper finds that the key to the violation of user privacy by commercial companies using facial technology lies in the fact that commercial companies collect users' facial data and other extended personal data without the user's consent and the user's knowledge, and use other personal data derived from users' faces for other purposes. Of course, all the purposes are based on the violation of users' privacy. It can be seen that the two elements of "without the user's informed" and "without the user's consent" are the key to the violation of user privacy by commercial companies. The principle of informed consent includes two small principles, one is the principle of informed, other is the principle of consent, and the principle of informed consent is the basis of the principle of informed consent in medical ethics. The principle of informed consent not only makes users pay due attention to the information, purpose, and use of facial recognition technology, but also pays attention to the "voluntary" and "non-mandatory" use of facial recognition technology by users.

2. Privacy invasion predicament of face recognition technology

The rapid development of artificial intelligence will undoubtedly make people's lives more convenient. At the same time, as the application of artificial intelligence in biometrics, facial recognition technology has brought about tremendous changes in people's lives along with smart mobile devices. An obvious example of this is that almost all smartphone manufacturers have added facial recognition modules to their mobile phones. The facial recognition technology in the facial recognition module can help users realize functions such as facial recognition unlocking and facial recognition electronic payment.

Facial recognition technology has been widely used in the following fields, such as video games, virtual reality, human-computer interaction, personal smart device and computer login, digital application login, mobile payment, Internet recording, video surveillance, electronic surveillance, suspects tracking, and finding lost children, etc. Facial recognition technology (machine recognition technology of face) can be generally expressed as: for the static image or video image of a given scene, the use of stored face database to identify or verify one or more people in the scene*(1)*. Of course, the above expression of facial recognition cannot fully summarize the characteristics of this technology. With the advancement of facial recognition technology, it has been possible to realize facial recognition for individuals in moving scenes to confirm their identity.

The ultimate purpose of facial recognition is to identify or verify the individual in the scene. Its main realization logic is to capture the stationary person or the moving person through the camera in the device with the help of intelligent devices, such as personal computers or mobile smart devices. Subsequently, the computer compares and verifies the personal facial features extracted from the scene with the personal facial information in

the background database. Finally, the system realizes the operation of facial identity recognition such as passing or rejecting. The current facial recognition technology relies on the related algorithms and technologies derived from machine learning and artificial intelligence, and with the rapid progress of technology, it realizes the iteration of functions and has developed to a very terrifying level. Specifically, most advanced facial recognition programs employ a type of neural network called a convolutional neural network (CNN). The system uses algorithms such as convolution to perform continuous complex analysis of images and even uses advanced analysis to identify people, animals, objects, or scenes*(2)*.

Are human faces completely incapable of replicating one-to-one? The answer may be no. Deepfake technology, born in 2017, may be able to challenge facial recognition technology. Deepfake technology was first used by hackers to create pornographic videos - replacing the female avatars in the videos with the avatars of their favorite celebrities. Deepfakes use a generative adversarial network called Gan, where an algorithm called a generator is fed random noise and turned into an image, which is then added to a stream of real images of celebrities. From this, it can be seen that Deepfake can create a face that is almost the same as a real person through AI algorithms and use it to deceive other people (maybe in the future will also deceive the facial recognition system). For example, hackers and other criminals use Deepfake technology to copy the target's face and pass the facial recognition system, then they can operate illegally as the "ghost" behind the real customer.

At the same time, facial recognition can be rendered useless by creating a "real" face, or by "sabotaging" the system. There's currently a tool called Bose that blocks certain facial recognition software from doing facial recognition. The tool can break facial recognition systems by adding other elements to the internet before uploading photos that look indistinguishable to the naked eye, but the hidden features hinder the detection system*(3).* If facial-faking technologies like Deepfake and facial-recognition attack tools like Bose continue to develop, they could cause widespread social problems.

The field of application of facial recognition technology can be divided into commercial applications and non-commercial applications. Usually, commercial applications necessarily have facial recognition technology built into various applications, and the facial recognition function is applied when the user uses the application. It's hard to imagine people abandoning facial recognition technology when faced with options that serve the same purpose. People often opt for facial recognition because it is fast and secure, allowing people to pay by pointing the camera on their phone screen at them. Non-commercial facial recognition applications are also emerging. Some of the best examples are technology companies, such as Baidu, Tencent, and Microsoft, which are developing apps to help find lost children. This kind of app is based on cloud technology and scans facial images to determine whether the child in front of the camera is the same as the missing child. At present, these companies have found some missing children through facial recognition technology. Baidu, for example, has successfully found the six-year-old abducted Fu Gui's loved ones 27 years after he was lost*(4).*

Facial recognition technology is widely used, making people feel as if their facial information and images can be used by software or commercial companies at any time. When people use some software or smart devices with facial recognition technology, this software or device will confirm through various reminders that the user agrees to let this software obtain their facial information and make reasonable use. However, some software, devices, or products from commercial companies do not tell users that they have taken facial information and used it for other purposes. For example, Facebook's facial recognition is enabled by default; Facebook's system works only if users choose to keep it as default. So in 2015, users in Illinois accused Facebook of violating the state's Biometric Information Privacy Act when collecting biometric data*(5).* Of course, Facebook users have discovered their facial information and filed a lawsuit to expose this unethical behavior to the public. However, some software or smart devices will turn on the device's camera without the user's agreement to obtain the user's facial information. Privacy consultant Dylan Curran claims Apps can

take photos and videos without telling users, run real-time facial recognition to detect facial features or expressions, and even stream cameras to the internet in real time*(6)*.

Some commercial companies have been able to identify the user's facial information through facial recognition technology and obtain additional personal information through the user's facial information. An Internet company called Clearview AI has developed a facial recognition software called Clearview, which can not only accurately recognize human faces like other facial recognition software, but also can use the recognized face or face picture to link to the location of the web page where the images appear, as well as a link to almost all of the person's publicly available images. The backbone of the system is a database of 3 billion images that Clearview claims to have scraped from Facebook, YouTube, Venmo, and millions of other sites, and it's far beyond anything the U.S. government or Silicon Valley giants have built. While proponents cite the use of the technology to prevent or deter crimes, including child sexual abuse*(7)*, the emergence of this software will also greatly increase other risks. For example, people can get relevant information about strangers by taking photos of them, and then entering the personal homepage of social networking sites to carry out harassment or abuse; criminals obtain photos of the school where the victim is studying through the software, to know the school of the victim, which is more conducive to criminals to carry out the kidnapping.

3. Personal privacy and facial ethics

Ethics has had a complex and protracted discussion of privacy. As to why privacy is important, one view holds that the value of privacy is intrinsic and ultimate, a condition and right inseparable from human dignity*(8)*; Another view holds that the right to privacy is not a fundamental right, because every violation of one's privacy is already a violation of some other rights*(9)*. The first view shows that privacy is essential for autonomy and protection of human dignity, this view is linked to human dignity; the second view, which shows that privacy is the basis of many other human rights, links privacy to other rights.

Philosophers have worked hard to define privacy, and the definition of privacy is often associated with the word "proximity." Michael J. Quinn thinks that the privacy people have is the right to allow areas that are inaccessible to others*(10)*. This definition can be expressed as: privacy enables us to create barriers and management areas to protect ourselves from unnecessary distractions in life, which enables us to understand who we are and how we interact with the world around us. When others violate our privacy, it violates the individual's right to freedom, especially the negative freedom of individuals. Isaiah Berlin argues that the subject (a person or group of persons) is allowed or must be allowed to do what he is capable of doing without interference from others*(11)*. If you simply summarize negative freedom, it is "freedom from...". Berlin believes that what the concept of negative freedom emphasizes is "not being interfered with by others", and the core of "not being interfered by others" lies in non-coercion, that is, the field where I can act in other ways, and there is no intentional interference by others. In other words, individuals are not artificially prevented from achieving a certain purpose.

As seen from the above examples of commercial companies invading individuals through facial recognition technology, these companies usually obtain personal facial information without the user's knowledge. Personal facial information is necessarily part of an individual's physical privacy. If an individual knows and agrees that a commercial company obtains his/her facial information and data through facial recognition technology, then this behavior can be regarded as a transfer of power, that is, an individual transfers his privacy rights to a commercial company. However, when the commercial company obtains the user's facial data and information without the user's knowledge, that is the commercial company violates the individual's right to maintain dignity, especially when the commercial company uses facial recognition technology without the user's knowledge. Other behaviors infringe other rights of users, including but not limited to negative freedom rights and portrait rights. Whether it is price discrimination and identity discrimination against users through facial recognition technology, or criminal activities caused by the disclosure of personal

information through facial recognition technology, it shows the violation of negative freedom caused by the abuse of facial recognition technology. To a certain extent, the right to portrait is also a kind of right to privacy, because both portrait and facial privacy use the face as the main carrier.

The rules to protect privacy enables us to assert our rights in the face of serious power imbalance, especially since the current commercial companies use various technical means to obtain our facial privacy without our permission. No privacy means we don't have the right to protect our facial information from being disclosed. When commercial companies use facial recognition technology to violate people's negative rights by invading privacy, there is no doubt that they are violating the iron law of "freedom from...". People all hope that they will not be treated unfairly, that they will not be prejudiced, and that they will not be harmed by the disclosure of their privacy.

However, it would be too simplistic to reveal the importance of privacy in facial recognition technology alone. After all, other science and technology also bring privacy problems, such as big data technology. In cyberspace, especially in the era of big data, loss of privacy can easily occur. The world's technology giants have all used big data technology to assist their business operations, such as Amazon, Alibaba, JD, etc. As e-commerce giants, Amazon and Alibaba usually use big data technology to "portrait" users to better recommend other similar products to users. When these e-commerce platforms implement price discrimination against users, big data technology must be used. Big data technology must obtain a large amount of data from users, including browsing history of products, purchase records, time spent on products, prices of browsed products, personal account number, ID number, contact information, etc. In the context of e-commerce, many consumers' personal information is collected without their knowledge, and consumers do not know what purpose the collected personal information will be used for.

It can be seen that when discussing the privacy issues of other technologies, including the aforementioned commercial companies' use of big data technology to violate users' privacy, although the means and methods of obtaining users' privacy are different from those of facial recognition (big data technology collects users' historical browsing records and personal information, facial recognition technology "scans" a person's face), the result is to recommend products and so on. Therefore, if we talk about privacy issues and the importance of facial recognition in this way, it must be no different from discussing other technologies. So what if the true privacy importance of facial recognition technology could be differentiated from other technologies? This paper believes that the biggest difference between facial recognition technology and other technologies, such as big data technology, is the human face, that is, the importance of facial recognition privacy must have its important ethical significance. In ethical terms, it has facial ethics.

A human face is a part of a person's appearance. The same hands, feet, height, skin color, and figure are all important signs to distinguish it from others. However, the biggest difference between a human face and other "human features" is that the face is individually identifiable, which means that if a person loses his torso, leaving only his head, others will still be able to identify "who you are". From this, it can be seen that the human face is one of the important elements of human self-existence, but the above analysis is only an analysis at the physical level and does not show people that the face is the philosophical foundation of self-existence.

Emmanuel Lévinas, a famous Lithuanian philosopher, has conducted an in-depth discussion on the relationship between ethics and the face. Therefore, this article will start with Levinas' theory to analyze the human face. The ethical significance of the face, especially the significance of the face to the existence of the self and its basis for the communication between the self and others. Levinas believes that the human face has a very upright state, and its sense of confrontation with exposure is defenseless. The skin on the face is the most exposed skin, which means that people's inner world can be fully presented through the face. Emmanuel Levinas said:

It calls to me above and beyond the given that speech already puts in common among us. What

one gives, what one takes reduces itself to the phenomenon, discovered and open to the grasp, carrying on an existence which is suspended in possession-whereas the presentation of the face puts me into relation with being. The existence of this being, irreducible to phenomenality understood as a reality without reality, is effectuated in the non-postponable urgency with which he requires a response*(12)*.

"It" here refers to a person's face. This passage shows that the face (face) is not only the embodiment of self-existence at the physical level but also the self-existence of the inner spiritual world. The face is the existence of the self at the physical level that can be understood by people without too much explanation. As mentioned above, when a person loses the body and only the face exists, others can also identify it, just like the identity card on the national identity card. Only the facial image is required as the only picture of the human body. Although the ID card also includes the ID number, the personal facial photo on the ID card is still the main basis for identifying a person. It is not difficult to understand that the face is the existence of the self at the physical level and the self-existence of the inner spiritual world.

What would you do if you were faced with a sad individual with a crying face? One might say, I'll ignore it, but most people will have the moral feeling of caring for that grieving person and will most likely talk to him because of primitive human sympathy. That is, as Niklas Toivakainen analyzes Levinas' Ethics of the Face, All our reactions to others are always about the other's "face." This suggests that morality is not about constructing a theory or extending morality (although this can be related to the general moral claims of the other party), but always about a dynamic of opening up to the other party, allowing the other party to touch us without limit, rather than running away from it, repressing /suppressing how the other person touches us, and how we respond to each other*(13)*. That is, in Levinas' view, the face is the origin of human discourse, the ethical relationship between the self and the other, leading to obligations from the self to the other. In this way, each is connected to others by being simultaneously self and as part of society as a whole. This also shows that the ethical significance of the face is that the face can reflect the existence or actual situation of the individual's inner spirit, that is, the face is the embodiment of self-existence, whether it is spiritual or material, and at the same time, the outside world (such as other people) can pass Facial features (such as crying) to show certain obligations to people, such as oral care. Therefore, it can be said that the face represents the dignity of the person, but also the moral obligation of others to the self. Therefore, facial recognition technology must ensure that the realization of personal existence and the external does not cause moral harm to the individual, such as an invasion of privacy. Especially in the digital age, with the widespread use of facial recognition technology, commercial companies or individuals (such as hackers) can obtain people's facial information through different means, and people will also upload their facial pictures to various digital media, such as Weibo, WeChat Moments, etc. People share and interact with others through their faces, as sending a laughing emoji on Weibo indicates that their psychological state is happy, then others will comment on it, or have a good conversation and communication; someone posts a crying face, others will show moral concern for him, or comfort him.

The above example is of course the external moral obligation to the individual, but Levinas' face ethics is not so simple. It shows that the face is a channel for external communication with the self, and the external should pay attention to the corresponding moral obligations of others, that is, the external do moral things to individuals. This paper believes that when facial recognition technology obtains personal facial information, individuals must not want others to conduct unethical behaviors on themselves, especially outsiders should not conduct evil operations on personal facial information and personal privacy information obtained through the face. That is, the problem is only how to understand the obligations of the self to others whose existence is complicated by their digital masking and creative appearance.

4. Discussion and conclusion

Informed consent is a principle of medical ethics applied to the medical field. Informed consent, that is, patients, have the right to know their

conditions and can decide on the prevention and treatment measures taken by medical staff, which has been widely accepted by the Eastern and Western medical circles and recognized by patients. The starting point is also patients' rights. The violation of user privacy by facial recognition technology can also be regarded as a violation of the user's rights. Of course, privacy rights are the most critical, but the right to obtain negative freedom cannot be ignored. This section provides a detailed analysis of why the principle of informed consent is important in facial recognition and how the principle of informed consent in medical ethics can be applied to the privacy issues of facial recognition technology.

Through the above case of how facial recognition technology violates user privacy, it can be deeply analyzed to discover how commercial companies violate the essence of user privacy. When people use some software or smart devices with facial recognition technology, this software or device will use various reminders to make users agree to let this software obtain their facial information and use it reasonably. But this is not all, some software, devices, or commercial company products do not inform users that they have access to facial information for other uses. At the same time, in addition to obtaining facial information without the user's permission, obtaining other information through facial information is also a reflection of the invasion of privacy caused by facial recognition technology. Some commercial companies have been able to identify users' facial information through facial recognition technology and use facial recognition technology to obtain additional personal information through facial recognition for other purposes, such as customer priority discrimination or price discrimination. It can be seen that the main manifestations of the privacy problems of facial recognition technology are divided into two types: first, commercial companies obtain the user's facial information without the user's consent or the user's knowledge; second, after obtaining the user's facial information through legitimate or improper means, the commercial companies can obtain other private information of the user through the facial information, such as identity, occupation, mobile phone, hobbies, etc. And without the user's knowledge or consent, the commercial companies engage in other commercial, non-commercial, legal, or illegal conduct. It must be pointed out that the latter must be based on the former, which cannot be achieved without facial recognition technology.

When people discuss whether science and technology are good or evil, they usually think that science and technology itself are neutral, and it is no good and evil. Therefore, people's evaluation of the good and evil of certain science and technology usually does not start from the technology itself, but from the subject who uses the science and technology. People interpret the problem as the fact that technology products have only extrinsic value*(14)*. This also means that when we analyze the problems caused by facial recognition technology When it comes to privacy issues, it is also possible to start from the main body of a commercial company, rather than simply from the facial recognition technology itself. Of course, it is not impossible to discuss the good and evil of facial recognition technology itself, what needs to be done is to analyze the good and evil of the intrinsic value of facial recognition technology. Philosophers distinguish two kinds of values: instrumental values and intrinsic values*(15)*. The former is the value that can bring other benefits, while the intrinsic value is good value in itself. For example, the tool value of facial recognition is that it can accurately identify the lost child and find the lost child through facial recognition technology. This is the value of external goodness.

Whether it is the first manifestation or the second manifestation of the facial recognition problem, what these two manifestations have in common is that the commercial company collects the user's facial data without the user's consent and without the user's informed and uses the user's facial information and other personal information for other purposes. It can be seen that the two elements of "without user consent" and "user unawareness" constitute the key for commercial companies to violate user privacy, and these two elements are also the basis for medical ethics to formulate the principle of informed consent. There are two main situations in which the patient's right to informed consent is violated during the implementation of medical behaviors: the first is the inability to understand the information provided

by the physician because of the inability to obtain true and comprehensive information or the limited level of cognition, and ultimately leads to the abandonment of this right; the second is that when the physician performs the duty of disclosure, the realization of the patient's right to informed consent is hindered due to the existence of bad motives. It can be seen that the violation of patients' rights in medical behavior has a potential commonality with the privacy problem of facial recognition. Therefore, we can improve the characteristics of the principle of informed consent in medical ethics (divided into the principle of informed and the principle of consent) concerning the privacy issues of facial recognition technology and take it as the main ethical principle to solve the privacy issues in facial recognition technology.

4.1 Informed Principle Application of Facial Recognition Technology

The informed principle means that users can know what they need, have full knowledge of the advantages and disadvantages of facial recognition technology, and can make rational judgments about their gains and losses. The informed principle does not require users to be completely rational, and it is unrealistic to be completely rational. The principle of knowledge is intended to explain that when users use facial recognition technology, commercial companies or other units must enable users to know the specific circumstances of facial recognition through various forms, including but not limited to setting up user terms for users to read. User terms or other forms that allow users to know must inform users of relevant information in their use of facial recognition, such as the user's facial information will be collected and included in the database; the user's facial information will be used for other operations, for example, it helps users to better purchase products (facial recognition technology can analyze users' preferences and allow commercial companies to recommend products to users through facial recognition technology). However, this is still not enough, especially for the emerging technology of facial recognition, users should also know the relevant information about facial recognition algorithms. Although, some commercial companies will claim that the facial recognition algorithm is a company secret, especially when the company's facial recognition technology is at the forefront of the industry. But there is a difference between technical trade secrets and the rationale and general design of an algorithm, which should be accessible to the public so that the public can fully trust the system*(16)*. That is, although the algorithms may be trade secrets to commercial companies or other individuals and are protected by laws such as intellectual property laws, the overall design ideas and philosophy of the algorithm must be disclosed to users, and users must be told some details of the algorithm (eg, whether the algorithm can automatically turn on the camera). This information is released to let most non-professional users know some of the details of the facial recognition process. All in all, users must be able to obtain sufficient information about facial recognition technology, and the facial recognition technology provided by commercial companies or other individuals has sufficient information and authenticity.

4.2 Consent Principle Application of Facial Recognition Technology

The key to the principle of consent is voluntary versus non-coercive. When individuals use various applications based on emerging technologies, or commercial companies use emerging technologies to achieve other purposes, users will not be required to sign a consent confirmation. With the emergence of smart devices, especially the popularization of smartphones, more and more people are concerned about whether people agree with commercial companies to obtain personal privacy information. Some companies may give some terms for users to read before users use related mobile phone smart software (some of this software rely on facial recognition technology), such as collecting personal mobile phone numbers, SMS records, mobile phone gallery, fingerprints, and other information. Users can use this software after confirming their understanding and agreement. However, it is worth noting that although some companies will give users access to these terms, this does not mean that users have the right to choose voluntarily, and sometimes it is mandatory. Because, some software is already set, not agreeing to the terms will not allow the user to start using the software. Therefore, it can

be seen that such terms have hidden "mandatory" because the user's "disagreement" with the terms will lead to the "unusable" of the software. Consent is closely related to informed consent. Logically speaking, consent must be established based on informed consent. Because the user is unaware of various circumstances, such as the purpose and means of facial recognition technology, the user must not consent. However, there is still a certain distance between reality and theory. Some commercial companies will not fully inform consumers of the specific purpose of facial recognition, the means of obtaining the face, and details (such as whether the camera is used privately, the general framework of the algorithm of facial recognition technology, and whether the privacy of users is violated) in the user terms. information about whether the user's privacy is infringed) is completely told to consumers; what's more, no information about facial recognition technology is given to users at all, as if facial recognition technology has become "invisible" between users and commercial companies, this results in users having no idea that they are a potential target for facial recognition technology. Therefore, the principle of consent must be able to effectively solve the above problems. This article attempts to summarize the principle of consent as, firstly, when commercial companies use facial recognition technology, they must let users know that they are using facial recognition through various means (such as user terms); secondly, users cannot be forced to agree to the terms of use (if they do not agree to the terms, they cannot use the software of facial recognition technology); finally, commercial companies cannot make individuals have the principle of consent to use (such as personal use of facial recognition technology must be prohibited in the absence of user terms for users to read and agree to).

It must be pointed out here that the principle of informed consent must be given to users or individuals by commercial companies. The principle of informed consent includes the principle of informed and the principle of consent, both of which must be satisfied. Moreover, commercial companies must first satisfy the principle of informed consent of users and then satisfy the principle of consent of users. The former is the basis of the latter. If these two principles cannot be satisfied, or only one of them can be satisfied, the function of the informed consent principle will be lost, and the privacy of users or individuals will still be violated.

Funding: This work was supported by the Western Project of the National Social Science Foundation of China (donation number 22XKS011).

Informed consent was obtained from all subjects involved in the study. According to national law, formal approval of this study is not mandatory. The authors declare no conflict of interest.

References

1. Zhao WY, Chellappa R, Philips PJ, et al. Face Recognition: A Literature Survey. *Acm Computing Surveys* 2003; 35(4): 399-458.
2. Frederick B. Facial Recognition [Internet]. *Technopedia*. 2022 [cited 2022 Jul 15]. Available from: https://www.techno-pedia.com/definition/32071/facial-recognition
3. ROBERTS JJ. Here's a New Way to Trick Facial Recognition [Internet]. *FORTUNE*. 2018 [cited 2022 Jul 17]. Available from: https://fortune.com/2018/06/13/trick-facial-recognition%20/?source=post_page----------%20-------&ref=hackernoon.com
4. aihot. Heartwarming Technology! Microsoft, Baidu Use Facial Recognition to Reunite Missing Families. [Internet]. *aihont.net*. 2017 [cited 2022 Jul 25]. Available from: https://www.aihot.net/application/4447.html
5. Stempel J. Facebook loses facial recognition appeal, must face privacy class action [Internet]. *REUTERS*. 2019 [cited 2022 Aug 1]. Available from: https://www.reuters.com/article/facebook-privacy-lawsuit-idINKCN1UY2C1
6. Day H. This is the terrifying reality of what happens when you give an app access to your camera and microphone [Internet]. *ShortList*. 2018 [cited 2022 Aug 1]. Available from: https://www.shortlist.com/news/app-access-camera-microphone-privacy-twitter-listening
7. Ina F. Clearview Brings Privacy Concerns from Facial Recognition into Focus[Internet]. *AXIOS*. 2020 [cited 2022 February 10,]. Available from: https://www.axios.com/2020/02/10/clearview-facial-recognition-law-enforcement
8. Allen AL. *Privacy Law: Case and Materials*. Beijing: Press of Chinese Democratic Legal System; 2004: 16. (in Chinese)
9. Richard V. Privacy as Life, Liberty, Property. *Ethics and Information Technology* 2003; (5): 199-210.
10. Michael JQ. Ethics for the Information Age. Beijing: Publishing House of Electronics Industry; 2016: 204. (in Chinese)
11. Isaiah B. Liberty. Jiangsu: YinLin press; 201:170. (in Chinese)
12. Emmanuel L. *Ethics and the Face*. Netherlands: Springer; 1991: 212.
13. Niklas T. Machines and the Face of Ethics. *Ethics and Information Technology* 2015; 18(4): 1-14.
14. Armin G. *Handbuch Techniketh*ik. Beijing: Social Sciences Academic Press (CHINA); 2017: 233. (in Chinese)
15. Joel R, Graybosch A. *Ethics and Values in the Information Age*. Beijing: Peking University Press; 2009: 276. (in Chinese)
16. Mikkel F. Machines and the Face of Ethics. *European Journal of Social Theory* 2015; 18(2): 168-184.

Received: January 30, 2023
Accepted: February 12, 2023