HiLL PUBLISHING

Journal of Humanities, Arts and Social Science, 2023, 7(10), 2067-2071
https://www. hillpublisher. com/journals/jhass/
ISSN Online: 2576-0548
ISSN Print: 2576-0556

Study of Informed Consent Rules in Face Recognition

Linxi Yang

Dalian Ocean University, Dalian, Liaoning, China.

How to cite this paper: Linxi Yang. (2023) Study of Informed Consent Rules in Face Recognition. *Journal of Humanities, Arts and Social Science*, 7(10), 2067-2071.
DOI: 10.26855/jhass.2023.10.029

Received: September 30, 2023
Accepted: October 29, 2023
Published: November 27, 2023

***Corresponding author:** Linxi Yang, Dalian Ocean University, Dalian, Liaoning, China.

Abstract

The advent of the era of big data is an irreversible trend. With the development of network technology, personal information has become closely integrated with various social fields, encompassing technologies for information capture, transmission, and storage. Daily applications, access to places, and face recognition technology play an indispensable role in various aspects. However, while enjoying the convenience brought by information technology, the protection of personal information also faces inevitable challenges. Informed consent rules are studied to address the issues that arise in the information society, such as the lack of sufficient information for individuals, unreasonable consent practices, and unclear handling of personal information dynamics. In order to address these shortcomings, the notification method in informed consent rules needs to be improved to effectively protect personal information. This will allow for better protection of personal information security while still utilizing the convenience provided by facial recognition technology in a reasonable manner.

Keywords

Personal Information Protection, Face Recognition, Informed Consent Rules

1. The risk of using face recognition technology

The issue of technical defects concerns the security and accuracy of face recognition technology. In terms of security, two-dimensional face recognition technology is less secure compared to three-dimensional technology, but it cannot be widely used at present due to the high cost of three-dimensional technology. In order to reduce costs, many technology users choose the less secure 2D technology, thus increasing the risk of impersonation. In terms of recognition accuracy, although face recognition technology continues to mature, there are still factors such as algorithm deviations, database information collection errors, light environment, and decorative object occlusion that may lead to recognition errors. Face recognition technology has concealment in the process of acquisition, and it can obtain the face information of the person concerned without contact, while the person concerned may not know and without prior consent or cooperation. This leads to an asymmetry in the mastery of information, especially in public places, where the collector can take advantage of face recognition technology to freely collect others' facial feature information, steal others' privacy, and pose a threat to the safety of the collected person (Zhang Xinbao, 2015). From the perspective of infringement consequences, any information has the possibility of leakage, but face information is unique compared with other information. Even if a user's personal information such as payment password or bank card number is accidentally known by others, the user can stop the damage result from happening or expanding by changing the password or freezing the account. However, once face information is leaked, it cannot be changed. Others can identify the information subject by accurately recognizing the facial information and obtain information such as race, skin color, mood changes, and even health status displayed by the facial features to commit forgery and

fraud. The impact this has on the information subject is irreversible, and even if remedial measures are taken afterward, the damage already caused cannot be repaired.

2. The Establishment and Status of the Informed Consent Rule

The concept of informed consent originally originated in the medical field to safeguard the patient's right to autonomy. In the 1914 U.S. case Schloendorf v. New York Hospital Association, the court made clear that "all normal adults have the right to decide what to do with their own bodies. If a physician performs a procedure without the patient's consent, he or she commits a tort and is liable for damages." With the development of biotechnology, the concept of informed consent is gradually being applied in the field of biomedical research to limit the excessive use of human tissue samples.

In the information age, the concept of informed consent is widely recognized internationally as an important tool in the field of personal information protection. Some scholars even believe that the concept of informed consent is the core principle of personal information protection. This concept is also actively reflected in personal information protection legislation in various countries, and rules for informed consent of personal information have been gradually established. The rule of informed consent of personal information requires that the processor of personal information can only process personal information after obtaining the knowledge and consent of the information subject. This rule is usually based on the behavior model of "informing and consenting" and focuses on ensuring that the information subject truly understands and consents to the information processor's actions.

The rule of informed consent for personal information essentially reflects the principle of individual autonomy in the field of personal information protection. In the information society, frequent handling of personal information seems inevitable, and personal information is directly related to personal rights and interests (Hu Wentao, 2018). Therefore, access to personal information, who obtains it, and how it is used should be determined according to the individual's wishes.

3. Problems with informed consent rules in face recognition in China

3.1 Lengthy terms and conditions - hidden character style terms

The total number of downloads exceeds trillions of times. The average time spent by users on various apps every day exceeds three-quarters of the total time spent on the Internet, which leads to a large amount of online behavior data being retained. Information processors, faced with such a huge amount of user information, need to spend a lot of time and resources to develop privacy policies and informed consent, conduct corporate compliance management, inform and disclose information to users one by one, and withdraw informed consent. As the cost of consent rises significantly, information processors are often busy informing every detail of the matter, preferring to adopt a formatted privacy policy. However, in practice, to avoid the hassle of informing users multiple times due to the different matters involved, platforms tend to inform information processing rules for basic services and information collection rules for additional services at once in the standardized privacy policy, resulting in excessive information content. It is observed that the privacy policies of Meituan, Taobao, Weibo, etc. even exceed 10,000 words, and the personal information protection policy of Ctrip even exceeds 20,000 words. If we add the links to the rules for protecting children's information, third-party SDK catalogs and fact sheets, and privacy policies of related derivative businesses, the length of the privacy policy becomes even more lengthy and complicated, further increasing the reading burden of the information subject, which eventually leads most users to actually skip the privacy policy and click "agree" directly.

3.2 Consent model is unreasonable

3.2.1 Consent Enforcement - Consent is required for use

Under current market conditions, "one-to-many" (e.g., one app for multiple users) has become the dominant method of collecting personal information. While screen clicks have become the means of expressing consent, changes in the interaction interface, notification methods, and consent methods pose challenges in determining the authenticity of consent.

First, the information collector, through its contractual advantage, leaves the information subject with a single-choice choice of "consent or leave". By virtue of their unique products and services or dominant market position,

online platforms have set up the "opt-in or opt-out" mode of choice. Once the information subject rejects the platform's collection of personal information, he or she is unable to use the platform's basic functions. In this case, the information subject is forced to consent, and the actual effect of the right to consent is weakened.

Secondly, the external availability of personal information leads to the loss of the freedom of refusal of the information subject. Refusal is a manifestation of freedom, but when the effect of refusal and non-refusal is almost the same, refusal loses its practical meaning. The powerful computing power of new network technologies such as big data and artificial intelligence makes the information subject's refusal irrelevant because the collector has the ability to infer the information subject's personal information from other information already obtained. Therefore, in the face of powerful computing power, refusal gradually loses its proper effect, and the value of consent becomes scarce as a result (Wu Hong, 2018).

3.2.2 Agreeing to extremes - agreeing in an all-or-nothing manner

Personal information can be divided into general personal information and personal sensitive information. Typically, additional services require a greater variety and detail of personal information to be collected and therefore require stricter informed consent in the authorization process. However, the reality is that information processors often do not distinguish between the types of businesses and services that require separate notification and enumerate information handling rules for all service functions in their privacy policies. Regardless of whether the information subject needs additional service functions or agrees to the collection of personal information for other purposes, he or she must ultimately click "consent. This blanket notification model is suspected of forcing consent, and even if the user reads the privacy policy, he or she cannot be truly informed.

In addition, most privacy policies provide for the sharing of collected personal information with affiliates or cooperating third parties without the consent of the data subject, unless the affiliates or cooperating parties want to change the purpose or use of the personal information. Affiliated companies include subsidiaries and holding companies, and cooperating third parties include advertising-type partners, suppliers of goods or technical services, and commissioned promotion partners. The scope of sharing is so broad that the risk of personal information leakage increases significantly, and the information subject cannot refuse such information sharing.

3.3 Personal information dynamics out of control

3.3.1 Time of consent unknown - Personal information stored permanently

Time of Consent Unknown - The permanent information subject of personal information has certain control over personal information, and throughout the process of processing and using personal information, the information subject has the right to dispose of his or her personal information, including withdrawal of prior consent. In the initial stage of giving consent, the information subject may not fully understand, and as the information processing progresses, the information subject gradually realizes that his or her information rights are threatened or does not wish to continue processing the personal information, he or she may theoretically exercise the right to withdraw and request the information processor to immediately stop the processing act. The right of withdrawal of consent reflects the information subject's autonomous decision on personal information and is characterized by personality interests, which can be regarded as the right of withdrawal under the personality rights system. Withdrawal of consent is not only a withdrawal of the expression of intent, because a legal withdrawal means that the contract is void ab initio, making the information processor lose the legitimacy basis for the processing behavior before the withdrawal. Therefore, the withdrawal of consent shall be understood as a right of revocation for the information subject. Withdrawal of consent neither presupposes actual damage nor has a retroactive effect, and its legal effect is that the information processor shall not continue processing personal information and shall delete the personal information stored before the withdrawal of consent. However, the process of withdrawing consent is not as convenient and accessible as choosing to consent. Some Internet platforms set the withdrawal option in a hidden location, making the withdrawal process complicated and cumbersome, and withdrawing consent means that the user will lose the right to enjoy the service. Some platforms do not even offer the right to withdraw consent at all and do not have a withdrawal option. When personal information is threatened with multiple uses, information subjects are caught in a dilemma, unable to choose again to consent or refuse, or effectively withdraw their previous consent. Storage.

Articles 16 and 17 of the Draft Personal Information Protection Law provide for the right of withdrawal of information subjects, requiring information processors to provide convenient ways to withdraw consent and not to refuse to provide services due to withdrawal of consent. These provisions undoubtedly help protect the validity of the

consent of the information subject, but in actual industry practice, the design of the option to withdraw consent and whether the information subject's right to withdraw can be fully realized remains to be verified.

3.3.2 Concealment of the flow of personal information

Most of the APPs require the personal information subject to click "I have agreed to the privacy policy" when registering, which is considered to be the personal information subject's authorization for the initial use of the APP. However, research shows that some APPs' privacy policies do not explicitly state the secondary use of personal information, such as the BMI Travel APP; some APPs place the secondary use-related content on lower-level pages of their websites. Most APPs put the matter of secondary use of personal information in the user agreement, and only a few put it in the privacy policy. This indicates that companies do not pay attention to obtaining authorization for the secondary use of personal information subjects.

It should be clear that although the user agrees to the initial utilization of the APP when registering, this does not mean that personal information can be shared with third parties. When making secondary use, the APP should again obtain the user's consent and be subject to the restrictions on the scope and manner of use in the original terms.

4. Solution

First, in the original rules, users had to agree to the platform's privacy terms in order to use the service, otherwise, they could not use it. The privacy clause authorized all rights at once, and the informed consent rule was exhausted after a single use. This means that users give blanket authorization to information platforms for their information. In order to improve the informed consent rule, the requirements inherent in the rule need to be made to evolve, and feedback provided to users on an ongoing basis (Wang Wenxiang, 2018). Users' lack of understanding of privacy terms and inability to effectively consent to them, as well as the lack of communication between platforms and users that leads to information asymmetry, are the root causes of the failure of the informed consent rule. The premise of the informed consent rule is that users are informed, and if there are problems with understanding, consent loses its meaning. This is the current situation caused by the Internet platform and users together.

Second, in the original rules, once the privacy clause is signed, the Internet platform hardly reminds the user of the collection and subsequent processing of information. This makes it difficult for users to know clearly where the information is going. Since users have a more urgent level of perception and concern about sensitive information and a greater need to know how the platform collects and uses such information, they may change their authorization later on after thinking about it when they face new situations (Shi Wenjing, 2019). For general information as opposed to sensitive information, general information has less impact on individuals and does not cause substantial harm to users themselves, but still requires constant reminders to achieve all-around protection of users' informed consent and to ensure that personal information protection is implemented. Regarding the time interval of mandatory reminders, it should be more closely for sensitive information, while it can be longer for general information.

Third, in view of the lengthy, cumbersome, and detailed content of the current privacy policy and the default checkbox practice of most platforms, there is a need to rethink how to formulate privacy policies to meet the inherent requirement of informed consent. Default consent is a major obstacle to the implementation of general privacy clauses and the protection of users' informed consent. In fact, many platforms place privacy provisions in a relatively obscure location with default consent, without informing or reminding users. The purpose of a general privacy policy is to allow users to learn or read it once and then apply it to all Internet platforms. This saves users' time and also reduces the development cost of the platform, as the platform only needs to inform according to its own attributes and characteristic business, and otherwise follow the generic privacy terms (Ding Xiadong, 2018). Developing a generic privacy clause not only effectively addresses the issue of default consent, but also allows for good enforcement of informed consent rules.

5. Conclusion

The protection of personal information is one of the topics often discussed in the Internet environment. There is a growing concern and discussion about the "information cocoon" phenomenon regarding the collection and use of personal information. On the Internet, it seems that all contents are related to your interests and concerns, and these contents really know you deeply, know your interests and preferences and make people feel that their information is bound up. The digital society is a big data society, and personal information has significant value as an important source of data. The collection and comprehensive use of information has become an inevitable trend. Proper use of

personal information can achieve a win-win situation for both the platform and the user, while also increasing social well-being. However, if used improperly, it will not only cause great harm to individual users but also may cause a catastrophic blow to the Internet platform.

References

Ding Xiaodong. The dilemma and the way out of private law protection of personal information [J]. Legal Studies, 2018(06):194-206.

Hu Wentao. The concept of defining sensitive personal information in China [J]. Chinese Jurisprudence, 2018(05):235-254.

Shi WJ. The principle of informed consent in the perspective of personal information protection [J]. Journal of Liaoning Public Security and Judicial Management Cadre College, 2019(01):89-94.

Wang Wenxiang. The Limits and Ways Out of Informed Consent as a Basis for the Justification of Personal Information Processing [J]. Journal of Southeast University (Philosophy and Social Science Edition). 2018(S1):142-146.

Wu Hong. The use and protection of personal information under the concept of trust [J]. Journal of East China University of Political Science and Law, 2018(01):22-36.

Xu Lizhi. The dilemma of applying the principle of consent in the processing of personal information and the idea of breaking it [J]. Knowledge of Library and Intelligence, 2017(01):106-113.

Zhang Xinbao. From privacy to personal information: theoretical and institutional arrangements for remeasuring interests [J]. Chinese Jurisprudence, 2015(03):38-59.