Research on User Privacy Security of China's Top Ten Online Game Platforms

Lan-Yu Cui, Mi-Qian Su, Yu-Chen Wang, Zu -Mei Mo, Xiao-Yue Liang, Jian He, and Xiu-Wen Ye(✉)

Yulin Normal University, Yulin, China

Abstract. The privacy agreement presented to online game users is the basic guarantee of the running of an online game. An online game platform can have access to users' private information by setting various mandatory clauses. This paper takes the ten most popular online game platforms in China in recent years as examples, using documentary analysis and quantitative analysis to analyze their privacy clauses. The research results show that there are loopholes in protection of users' private information by online platforms that have gained access and rights to use them. Based on this, it is conducive to the protection of users' private information through improving information security protection system of online game platforms, adding the option for access denial of privacy information in the process of user registration, and mandatorily prolonging the time assigned for users to read the privacy agreements.

Keywords: Online game · Rights of privacy · Format clauses

1 Preface

The security of online games has become a frequently seen issue in network tort liability disputes and network service contract disputes. The premise for users to register for access to online game platform services is to accept the User Agreement and Privacy Policy provided by the platform. The content of these agreements is usually the format clauses prepared by online game companies in advance, which involves disclosure of personal identity information such as the users' name, ID, E-mail address, and head photo and so on. To wish to have access to the services, user can only passively click the "Agree" button to accept the terms. If online game companies do not protect the users' privacy, and the identity information is leaked, it will undoubtedly lead to the damage of the users' privacy. As a result, how to standardize the format clauses of online games is really important. Research on the user privacy agreements of China's top ten online game platforms can help deepen the understanding of the privacy security problems of Chinese online game platforms and improve the protection of users' private information on online game platforms and propose solutions accordingly.

Z. Deze et al. (Eds.): BDTA 2020/WiCON 2020, LNICST 371, pp. 168–175, 2021.
https://doi.org/10.1007/978-3-030-72802-1_12

2 Status Quo of Privacy Security on China's Top Ten Online Game Platforms

The privacy agreements of China's top 10 online game platforms are collected from their official websites and coded (see Table 1).

Table 1. Privacy agreements of China's top ten online game platforms

No.	China's top 10 game platforms	Code
1	GOG Privacy Agreement	A1
	GOG.COM User Agreement	B1
2	Origin Privacy Agreement	A2
	Origin Agreement	B2
3	Steam Privacy Agreement	A3
	Steam Subscriber Agreement	B3
4	Uplay Privacy Policies	A4
	splnproc1703	B4
5	WeGame Statement on Protection of Children's Privacy	A5
	WeGame Privacy Guidelines	A5-1
	WeGame Software License and User Agreement	B5
6	Blizzard Battlenet Privacy Policy	A6
	Blizzard Protection of Minors	B6
	Blizzard Battlenet End User License Agreement	B6-1
7	Cubejoy Privacy Protection Policy	A7
	Cubejoy User Agreement	B7
8	Nintendo Privacy Agreement	A8
	Nintendo User agreement	B8
9	Sguo Privacy Agreement	A9
	Sguo Service Agreement	B9
10	Netease Privacy Agreement	A10
	Netease User Agreement	B10

Based on the privacy agreements of China's top ten online game platforms, this paper analyzes the format clauses involving usage of users' identity information. It can be seen that in China's top ten online game platforms, users' e-mail address and username are used respectively. A1, A2, A3, A5, A5-1, A6, A8, A9 and A10 all include provisions on child protection, while A4 and A7 do not have relevant provisions. A3, A5 and A8 do not require users to be older than 16. For example, A3 has clearly shown in its agreements that the minimum age for registering a steam user account is 13, a restriction tougher

than before. B6 requires minor users to conduct real name authentication. A1, A2 and A3 do not mention the collection and use of users' mobile phone numbers while the agreements of the other seven game platforms have clearly pointed this out. A6, A7, A9 and A10 include clauses involving the use of ID information of users. A3 indicates that when setting up a user account, a number ("steam ID") will be automatically assigned to the account, without requiring providing or using a real name. The number will be used to refer to the user account, but it is stressed that the users' private identity information will not be directly exposed. Similar content does not exist in corresponding agreements provided by other game platforms. A9 doesn't mention the use of users' name, while Steam clearly points out that the users' name will not be used for the user account with the other eight game platforms saying that they will use the users' name for their accounts. Eight of the ten platforms use the users' date of birth. A6 requires to obtain information about the users' age, date of birth, gender and other non-private information, while the agreements of A7, A9 and A10 do not mentioned this part. A1, A2, A3, A5-1, A8 and A10 all include contents about the users' account avatar, while A4, A6, a7 and A9 do not have similar provisions on this issue. Statement released by A5 indicates that children should not upload real portraits as avatars when accessing the platform's services, while other agreements do not have such provisions. Except A9, all of the other online game platforms require users to share their geographic locations. For example, in A3, Steam requires information about users' geographic location to deliver content through the use of distributed server system. As for data sharing, however, A1, A2, A3, A5, A6 and A10 all agree to purchase content through third-party platforms that share direct connected account information through the use of relevant direct connected account information. On top of that, four of China's top ten online game platforms are not developed by Chinese companies, and the agreements of A1, B1, A2, B2, A8, B8, A9, and B9 are not formulated exclusively for Chinese users but for users worldwide. Online game platforms will encrypt the users' account and password information after collecting it, in case users forgets their password and cannot log in. It can retrieve the password through e-mail verification of identity information. (see Fig. 1).

Among all private information collected, the mobile phone number and E-mail address have to be provided by users to access the platforms' services, which users will need in registering an account and setting a password and username. Apart from that, in order to meet the demands for user identity verification and service security, platforms will also require users' ID card number, name and facial information, which is relatively more important identity information for users. If this kind of information is accessed by the platforms but not well protected, its leakage will lead to the infringement of users' privacy. In order to provide more personalized services to users, some platforms will collect the date of birth, avatar and other contents of the users. None of these platforms mention the restrictions on the use of real minors' portraits except Statement in A5, and such information is not prerequisite to use services. Additionally, these platforms share a feature, that is, users' information may be changed by Cookies. Moreover, Cookies are not bound by privacy agreement, so users' information cannot be guaranteed after being used by a third party. The abuse of identity information of users,

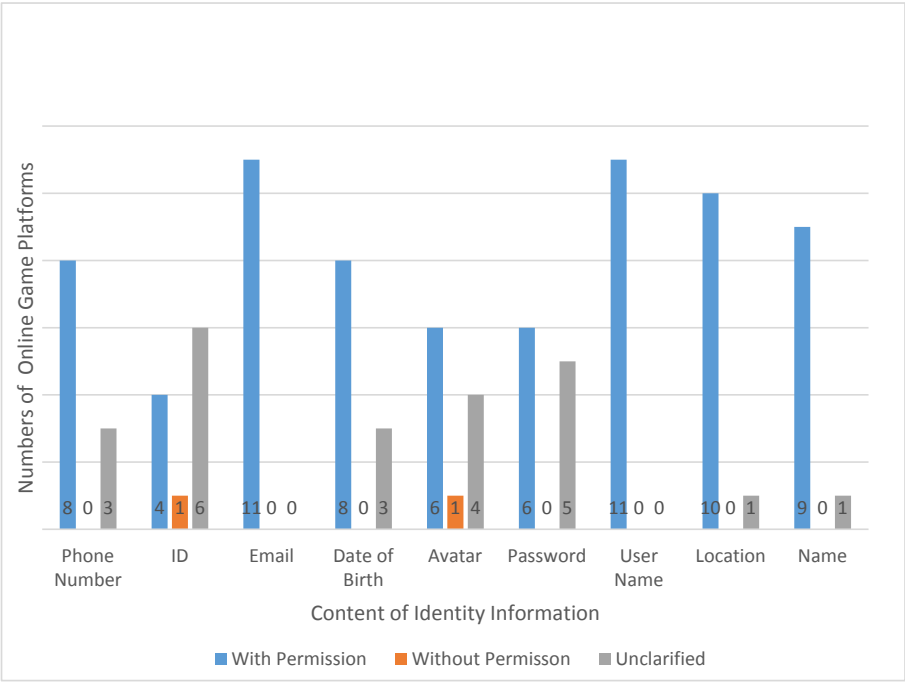

Fig. 1. Identity information required by agreements from China's top 10 online game platforms

especially of minors, may lead to the infringement of their privacy rights. If their information is leaked, it may be purposefully collected by lawbreakers, subjecting minors who have not maturely developed physically and psychologically to mental damage.

3 Research and Analysis

Through research and analysis on China's ten most popular online game platforms, it is shown that game platforms need to collect personal or non-personal information of users such as mobile phone number, avatar, geographical location, device information, etc. to provide their services, such as improving experience of reality in the game, limiting illegal behaviors and helping minor avoid addiction to games. Although personal information has not been collected excessively, the risk of personal information being abused due to the leakage still exists. Among the ten online game platforms, A3 and B3 clearly point out that the users' name would not be used to set up the users' account, while the other eight game platforms have a different policy. However, A1, A2 and A3 do not include collection of the private information and use of mobile phone number, which is, however, covered by the agreements of the other seven game platforms. Moreover, A6 needs to collect users' age, date of birth, gender and so on, but the agreements of A7, A9, A10 and other game platforms does not have similar provisions. Agreements of A2, B2 and A4 belong to foreign game platforms, whose common feature is that they require less from common users but include more provisions particularly for special

groups such as heart patients or minors. For common users, these agreements all say that their information will be shown to a third-party company called Cookie. Although the company has an agreement with the game company ensuring that it will not abuse or disclose the users' information, there is no valid evidence to prove it. However, Article 11 of China's "Network Security Law" stipulates that, the use of private information collected by network operators should be fair, just and open upon agreements of the information holder and collection of information unrelated to their services should be comply with the laws, administrative regulations and the agreement of both parties. Using private information should comply with the provisions of laws, administrative regulations and agreements with users to handle private information properly. However, this can only be applied for Chinese online game platforms, with foreign ones not bound in their privacy agreements. Based on the identification information collected, the ten platforms share this fragmentary information with the third party, creating a loophole and posing a threat to the protection of user privacy.

Although the platform only collects fragmentary personal information, it cannot guarantee that zero leakage. Zhou (2013) said that information leakage equals to the integration of fragmentary information. Game companies collect user information differently. For example, in terms of sharing data in China's top ten popular online games, A1, A2, A3, A5, A6, A10 agree to use the relevant direct account information to allow them to purchase content from a third-party platform. It is true that not all companies collect all aspects of personal information such as name, address, E-mail and so on, but it is possible that scattered information can be gathered s through sharing between third-party platforms or game company platforms, which is highly likely to lead to leakage of user information. In the case of Li Hanbin and Li Yuehua, the Appellants at Maoming Intermediate People's Court in Guangdong Province, Xie Jingdong, the defendants in the original trial, illegally sold citizens' private information through the Internet. This constituted the crime of infringing citizens' private information. The case shows that after the identity information is leaked, lawbreakers may take the opportunity to sell their information illegally, leading to abuse and exposure of personal information.

According to Jiang and Zhang (2012), there are security risks in the personal privacy of online games. There is a lack of restraint in preventing online game operators from selling or leaking users' personal information. Compared with anonymous users, real name users have relatively larger losses. After the real name system of online games, this disadvantage has become more obvious, not only in China, but also in foreign countries. Amanda and Mike (2020) pointed out that "organizations have been increasingly using information technology (IT) to enhance business operations and decision-making processes and thus information security is one of the most pressing issues facing organizations worldwide, influencing organizational sustainable information systems and business continuity. However, many managers and employees do not pay sufficient attention to information security issues in their organizations. As a result, the computer systems of most organizations are far less secure than they should be, and damages due to information security breaches are on the rise". Although this is a description of information leakage among enterprises' employees, it is similar to personal information leakage of Chinese online game platforms. It can be seen that the leakage of identity information of Internet users is a problem that cannot be ignored. In the age of big data, fragmented

identity information may also be integrated, leading to its illegal sale and abuse, and its leakage by the third-party platforms also aggravates its risk of abuse.

4 Suggestions on Users' Privacy Protection of Online Game Platforms

4.1 Suggestions for the Regulatory Bodies of Online Game Platforms

China's Internet platforms are supervised by Ministry of Industry and Information Technology of P.R.C, State Administration for Market Regulation, Internet Society of China and other departments. In order to achieve the best supervision effect and prevent the information leakage of internet users, the regulatory bodies themselves should first follow the principles of law enforcement, and not abuse their power to punish, or cover up the online platforms because of their illegal collection and sale of users' identity information for the purpose of profit. Secondly, they should limit and manage the content of user identity information collected by online platforms at different levels. Through the investigation and statistics of the information required by the developers of each platform and the feedback provided by users voluntarily, the regulatory bodies can formulate the format clauses for collecting personal identity information in the agreement of game platforms and specify the content of information that can be collected. Meanwhile, the platforms can be required to improve their technology of information security protection, and manage the crucial and the less crucial identity information at different levels to avoid the risk of excessive collection and information leakage. Finally, they should also consider the domestic users on foreign game platforms, strictly formulate the access mechanism of foreign platforms and restrict the cross-border transfer of personal information to better protect the identity information of domestic users.

4.2 Suggestions for Game Platforms

Platforms should strengthen the refinement of format clauses, set the minimum time limit for reading these clauses, highlight their options, and reduce the unnecessary clauses unilaterally beneficial to the platform side. The collection of users' ID, telephone number, E-mail address, head photo, date of birth, name and other information must be approved by the user first, protected and legally used. If the platform cooperates with a third party, it is necessary to inform the users in advance and emphasize the interest involved through words. Except that it shall not disclose the users' information, it has the obligation to guarantee that the third party acts in the same way. Zhang (2019) mentioned that the personal information right is positive on right holders, and they can request the actors to change or delete their personal information when it has been collected and used without permission. Therefore, a denial option should be added in the process of users' permission for platform services. At the same time, for users who have refused to fill in the unnecessary personal information on the platforms, services should be provided as well. Wang (2020) found out that some online game platforms have separate terms in their network service agreement with the privacy policy included. It is clearly stipulated that the users' consent to the network service agreement is regarded as the acceptance of their

privacy policy, too. This practice should be changed. The platforms should separate the privacy agreement from the service agreement, and get the users' personal information only after obtaining their consent to the privacy policy. Moreover, the minimum age of game users and time limit of playing games should be promoted among platforms. For registration, users need to use their real names, ID, and face recognition which will also be carried out regularly in the later stage. The real name registration also ensures the security of game transactions, and the minimum age, face recognition and time limit reduce the excessive exposure of minors to games, protecting their rights of education as well as physical and mental health. At the same time, the game platforms can establish a database for regular information management of ordinary users, and protect the key information of special groups. In pursuit of economic benefits, they should also reflect their social values to ensure the privacy and security of users' information.

4.3 Suggestions for Users

The types of users online are adults and minors, respectively. Chen (2018) believed that mature adults need to change their concept of negative power (i.e. hoping that their privacy will not be leaked by others, and being accustomed to putting themselves in the passive and defensive positions), so as to improve their abilities of personal information protection. On the one hand, when the users log in to a game, they should pay attention to whether the information to be filled in is reasonable or necessary, such as race, religion, marital status, political inclination and other sensitive information unrelated to the use of the game. If the platform still requires such information, the users can send opinions to platform or feedbacks to the regulatory bodies due to the excessive collection of personal information. On the other hand, the users should not click the links that pop up in the process of game running or the links sent by other players on the Internet, so as to prevent law breakers from embedding Trojan Horse into computers to steal users' identity information. As minors, they should follow the age rules stipulated in the agreements of game platforms. Those under the age should register and use the platforms under the guidance of their parents. In addition, parents should educate the minors on online security, and tell them not to trust other players in the game easily, so as to avoid the leakage of personal and family identity information due to their ignorance.

5 Conclusion

The identity information of online game users is an important part of their right of privacy. It is the responsibility of the online game platforms to protect their users' identity information from being leaked. It is also of great significance to the protection of users' privacy and the healthy development of online games. Therefore, the regulatory bodies of online game platforms are required to exercise their rights in accordance with the law, improve their regulatory system, as well as standardize and restrict the format clauses of the platforms; the online game platforms shall collect and use the identity information with the consent of the users, refines the format clauses and strictly performs their security obligations; online game users should strengthen their awareness of security protection of personal information, and take reasonable measures when their privacy is

violated. As for minors, they can use the platforms in a proper way. When the three parties join hands and work together, the privacy of online game users can be protected and the sound development of online games can be promoted.

References

Chu, A.M.Y., So, M.K.P.: So organizational information security management for sustainable information systems: an unethical employee information security behavior perspective. Sustainability **12**(8), 3163 (2020)

Chen, T.F.: Research on legal issues of privacy protection under the new media environment. Fudan Univ. **76** (2018)

Jiang, Y.Z., Zhang, P.: Analysis on the legal issues of the real name system of online games. Wuhan Univ. J. (Philos. Soc. Sci.), **65**(01), 55–58 (2012)

Wang Y.G.: On the effectiveness of network privacy policy–focus on the protection of personal information. Comp. Law Res. (01), 124–138 (2020)

Zhang, L.: Research on trace information protection of personal network activities–comments on the first case of privacy dispute over cookie in China. Hebei Law Sci. **37**(05), 135–150 (2019)

Zhou, S.Q.: On misuse and safeguard of personal information in the network crowd movement. Soc. Sci. Beijing **123**, 13–18 (2013)