Research on User Privacy Issues in VR/AR Class Mobile Apps

Zihao Xiang

Abstract:

With the rapid development of the Internet, an increasing number of devices are interconnected through the Internet, making the protection of user privacy during the information transmission process increasingly prominent. This paper categorizes user privacy issues into computer and mobile devices and analyzes their specific threats. Towards the end of the article, we propose methods for protecting user privacy from three perspectives.

Keywords: Security and privacy, Data anonymization and sanitization. Social network security and privacy.

1. Introduction

Communication has become a convenient affair in an era where all devices are interconnected. Internet users can easily exchange and transfer information using computers or mobile devices (like smartphones). On the one hand, computers and other mobile devices have built-in sensors that capture location, image, sound, and other information, which can automatically collect information about the user and their surrounding environment. After analyzing and processing this information, users' private data can be obtained. When users operate software on these devices, they also record their private data, leaving their privacy footprint on the device.

Every day, billions of devices collect and record users' daily lives and behaviors. A large amount of data generated in this process is discarded or sent back to companies as feedback data. However, neither the companies nor the users can properly manage this vast amount of data, leading to numerous system and data vulnerabilities. This allows attackers to steal improperly processed information, thereby endangering the data security of both users and companies.

Scientifically handling this user data is a challenging and detailed task. On the one hand, software companies need to define user data: which data can be discarded without processing, which needs to be encrypted or randomized before being discarded, and which includes private user information that must be securely protected. On the other hand, software companies also need to study the hardware information users use. They must design different privacy protection methods for different devices, providing comprehensive and accurate protection of users' private information.

In this paper, we have conducted a detailed study of the current issues related to user privacy protection. Through research, we have categorized privacy issues on electronic devices into computer and mobile devices, representing two important aspects of daily work and life. Subsequently, based on our research, we have classified user privacy information on computer and mobile devices into user-initiated retention and automatic recording. Finally, we have provided recommendations for protecting user information from three perspectives. Our contributions can be summarized as follows:

1. We researched user privacy information from both computer devices and mobile devices.
2. We conducted a thorough analysis of the content of user privacy information from the perspectives of user-initiated retention and automatic recording.
3. We provided multifaceted recommendations for the protection of user privacy information.

2. Related Work

2.1 User Privacy on Computer Devices

On social media, massive amounts of data are collected by media companies, either intentionally or unintentionally, and this data is further analyzed to ascertain user needs more accurately [1]. For example, user-generated data offers researchers and commercial partners opportunities for studying and understanding individuals on an unprecedented scale [2,3]. This information is crucial for online providers to offer personalized services; the absence of such data could lead to a decline in the quality of these services [4]. Meanwhile, due to the richness of the content, users may unknowingly or knowingly leak their privacy while using these platforms [5,6]. Such data can be exploited for malicious activities, posing potential user risks, including attacks from individuals and organizations. Many social media apps reveal more sensitive user data, such as home addresses [7] and personal preferences [8]. Although this private information is not directly exposed, it is subtly leaked, which is equally unacceptable to users.

2.2 User Privacy on Mobile Devices

The same issues exist in the realm of mobile app methodologies. Firstly, system permission management involves acquiring a lot of information permissions, which often relate to user privacy. Not every mobile app developer possesses a strong awareness of information protection, leading to developers unintentionally confusing or excessively requesting unnecessary permissions [9]. Users, often lacking a clear understanding of the accessibility of their personal information, tend to allow apps to collect all the information they need [10]. Researchers have extensively studied these issues. For instance, some have proposed dynamic permission granting methods [11], which restrict information access in apps and timely prevent data acquisition when certain privacy is not needed. Additionally, machine learning-assisted methods have been used to identify malicious software's information requests.

3. User Privacy

Users' privacy concerns encompass computer and mobile devices, indispensable parts of human learning and living. However, the privacy aspects that need protection in these two types of devices still differ.

3.1 Privacy on Computer Devices

Computer devices handle most office tasks and entertainment activities, involving a vast amount of personal information. After conducting surveys and categorizing, we have divided the information in these devices into ten categories, as shown in Table 1.

Table 1

Information types	user-initiated retention	automatic recording	content
Personal Identification Information (PII)	☑		Names, addresses, phone numbers, email addresses, identity card numbers, social security numbers, birth dates, etc
Financial Information	☑		Credit card numbers, bank account information, investment records, income and tax information, etc.
Health Information		☑	Medical records, health insurance information, prescription details, etc., are usually subject to more stringent privacy protection regulations.
Internet Activity	☑	☑	Browsing history, search history, shopping records, social media activities, geographical location data, etc.
Communication Content	☑	☑	Emails, instant messages, video and voice call records, social media posts, etc.
Work and Education Records	☑	☑	Professional resumes, academic papers, research data, examination scores, etc.
Biometric Data		☑	Fingerprints, facial recognition data, voiceprints, DNA information, etc.
Usage Habits and Preferences		☑	Device usage habits, software preference settings, customized advertising data.
Cybersecurity Information	☑		Passwords, encryption keys, answers to security questions, etc.
Device Information		☑	Hardware serial numbers, IP addresses, MAC addresses, operating system and software version information, etc.

We categorize the privacy on computer devices into two types: user-initiated retention and machine-automatic recording. User-initiated retention includes Personal Identification Information (PII), Financial Information, Communication Content, Work and Education Records, and Cybersecurity Information. On the other hand, machine automatic recording encompasses Health Information, Internet Activity, Communication Content, Work and Education Records, Biometric Data, Usage Habits and Preferences, and Device Information. Both types of information can lead to the leakage of crucial user data, providing opportunities for malicious actors.

3.2 Privacy on Mobile Devices

Mobile devices, characterized by their portability and high personalization, have seen an increase in the types of information they can collect due to advancements in mobile communication technology and the widespread development of mobile devices (including electronic wristbands). This leads to a richer array of user privacy information involved. As shown in Table 2, we have summarized the types of privacy information found on mobile devices.

Table 2

Information types	user-initiated retention	automatic recording	content
Contact information	☑		Names, phone numbers, email addresses, etc., are stored in the mobile phone contact list.
personal communication records	☑		Text messages, call logs, emails, social media messages, etc.
Personal media files		☑	Photos, videos, audio recordings, etc.
location information	☑	☑	GPS data, location history records, information on applications that use geolocation services, etc.
application data	☑	☑	Installed applications and their usage data, purchase records, in-app activities, etc.
Internet activity records	☑	☑	Browser history, search records, cookies, autofill data, etc.
biometric data		☑	Fingerprints, facial recognition, etc.
device information		☑	Model, operating system, unique device identifiers (like IMEI), SIM card information, etc.
health and fitness data	☑		Step count, exercise records, heart rate data, sleep monitoring data, etc.
financial information		☑	Banking app data, electronic payment records, credit card information, etc.
work-related information	☑		Emails, work documents, meeting records, etc.

Similarly, we categorize personal privacy information on mobile devices into user-initiated retention and machine-automatic recording. User-initiated retention includes contact information, personal communication records, personal media files, internet activity records, biometric data, and work-related information. Machine automatic recording includes location information, application data, internet activity records, health and fitness data, and financial information.

4. Impact of User Privacy Breach

Based on the analysis in the previous sections, user privacy faces different types of leakage on different devices. In this chapter, we will further explore the impact of user information leakage on individuals and society.

4.1 Individual Users Impact

Identity Theft. Personal privacy leaks can lead to malicious actors using other people's identities for various activities. This includes the theft of sensitive information, impersonating the leaked user in social activities, and causing harm to their reputation. Attackers may use stolen user accounts on social platforms to solicit more personal information from their friends or engage in financial fraud. In many apps, identity thieves with access to a large amount of stolen personal information can be difficult to detect by other software, which can severely disrupt the lives of the victims.

Personal Security Threats. After obtaining personal information, malicious individuals may pose personal security threats to the victims. This can include physical attacks based on their home addresses and communication attacks via phone. For public figures or individuals in specific professions, such attacks can significantly impact their reputation and safety.

Psychological Impact. Victims of privacy breaches often experience psychological health issues such as anxiety, unease, or depression. The deliberate threats made by perpetrators can lead to long-term psychological stress. Additionally, due to a lack of trust in others, victims of theft find it difficult to seek resolution through psychological counseling or other means.

Legal and Compliance Risks. Personal privacy includes highly personalized information, and disclosing personal privacy can lead to legal issues for individuals in sensitive professions. The impact can be even more significant if the stolen information includes sensitive legal documents or other critical data.

4.2 Social Impact

Decreased Overall Trust. To safeguard their information from potential misuse, people must exercise greater caution when interacting with users on social platforms. When the public faces scenarios where their information can be easily stolen, they become more wary of using and trusting social platforms and other devices and software that may be susceptible to information leaks. This can significantly reduce overall societal trust.

Hindrance to Technological Innovation. Frequent information leaks force device and software manufacturers to reconsider their marketing strategies and development directions. Software developers may have to develop privacy protection programs independently without a unified approach to address privacy breaches. This not only slows down overall development but also has the potential to create a more chaotic software ecosystem, hindering further technological innovation.

5. How to Protect Privacy

As discussed earlier, user privacy protection is crucial for device manufacturers, software companies, and individuals. We will now explore how to protect user privacy from these three perspectives:

5.1 Hardware equipment manufacturers

Physical Security Measures. In the realm of hardware device manufacturing, the integration of physical security features plays a pivotal role in fortifying device integrity. Manufacturers incorporate various safeguards into device designs, including tamper-resistant packaging and secure boot processes. These measures are purposefully implemented to thwart any unauthorized physical access attempts. By doing so, manufacturers ensure the device's physical integrity and bolster its resilience against potential breaches. This proactive approach to physical security underscores the commitment to safeguarding user data and device functionality.

Encryption Chips. Specialized hardware encryption chips, exemplified by Trusted Platform Modules (TPM) and Hardware Security Modules (HSM), are pivotal in enhancing data security. These dedicated hardware components securely store and manage sensitive information, including passwords and encryption keys. By utilizing encryption chips, software companies, and device manufacturers bolster the confidentiality and integrity of stored data. This hardware-based security approach provides a robust defense against potential breaches and unauthorized access to critical information, thereby augmenting overall data protection measures.

Supply Chain Security. Effective supply chain security management is imperative for ensuring the integrity of the components and software utilized in the manufacturing process. Software companies and hardware manufacturers must diligently assess and mitigate supply chain risks. This includes meticulously scrutinizing suppliers and vendors to ascertain their adherence to high-security standards. Organizations can fortify their defenses against potential vulnerabilities introduced through the supply chain by imposing stringent requirements and monitoring supply chain partners. This proactive approach is instrumental in upholding the overall security and trustworthiness of the end product, minimizing potential risks associated with the supply chain.

5.2 Software companies

Data Minimization. Data minimization is a critical principle that software companies must adhere to in data privacy. It mandates that these companies should only collect and process user data essential for their software's core functionality. Doing so reduces the volume of stored and processed data, thereby lowering the risk of data leaks and privacy breaches. This practice enhances data security and aligns with ethical data handling practices and regulatory compliance.

Regular Security Audits and Testing. In software security, regular security audits and penetration testing hold paramount importance. Software companies are urged to consistently perform these assessments to proactively identify and address potential security vulnerabilities. Security audits involve a comprehensive review of the software's code, infrastructure, and configurations, while penetration testing simulates real-world attacks to pinpoint weaknesses. By embracing these practices, software companies bolster their ability to fortify their applications against security threats, maintain data integrity, and ensure the trust of their user base.

Data Access Control. Effective data access control is imperative for safeguarding sensitive user information within software systems. Software companies should implement stringent measures to restrict internal access to user data, ensuring that only authorized personnel can access and handle this valuable information. Access control mechanisms deter unauthorized access and allow for the meticulous monitoring and recording of access activities. This proactive approach helps promptly identify and respond to suspicious or unauthorized access attempts, thereby fortifying the overall security of the system and upholding user privacy.

Feedback and Transparent Channels. In the context of user privacy, establishing channels for user feedback and complaints is indispensable. Software companies should provide accessible avenues for users to express their concerns and provide feedback regarding privacy-related matters. Additionally, transparency in communication is paramount, particularly when implementing changes to privacy policies. Companies must ensure that users are informed about any alterations to privacy practices clearly and comprehensively. This commitment to transparency fosters trust between users and software providers, allowing for a collaborative approach to privacy enhancement and compliance.

5.3 Users Themselves

Strengthen Password Security. Many users use the same password for different accounts, posing a significant security risk. It is essential to employ complex and unique passwords for each account and regularly change them to address this issue. Additionally, considering the widespread tendency to reuse passwords, it is highly recommended to utilize a password manager. A password manager helps users generate and securely store complex, distinct passwords for various accounts, ensuring security and organization.

Exercise Caution. Exercising caution is vital when sharing personal information on social media and other online platforms. This includes birthdays, addresses, and information about family members. It's important to be mindful of the information you disclose online, as cybercriminals and malicious actors often exploit personal data for various purposes. Therefore, it's advisable to limit the amount of personal information shared online and only provide such details when necessary while being aware of the privacy settings on these platforms to control who can access your information.

Understand Privacy Policies. Understanding Privacy Policies is crucial in safeguarding your personal information when using new services or applications. It's important to take the time to thoroughly review and comprehend the privacy policies of these platforms. Users can understand how their data is collected, processed, and protected. Privacy policies typically outline the practices and procedures organizations follow regarding user data, including whether they share it with third parties, how they secure it, and how they handle user consent. Being informed about these policies empowers them to make informed decisions about the services and applications they use and whether you are comfortable with their data handling practices.

6. Conclusion

This paper appears to be a summary or introduction to a research paper on user privacy in computer and mobile devices. It outlines that the research has conducted a detailed and comprehensive study on user privacy issues in these devices. The study includes definitions of privacy, the impacts of privacy breaches, and privacy protection methods. It also mentions that the research analyzes privacy protection from the perspectives of hardware device manufacturers, software companies, and users. We will explore specific types of privacy protection issues in future research.

Acknowledgments

Reference

[1] Joseph Bonneau, Jonathan Anderson, and George Danezis. 2009. Prying data out of a social network. In Proceedings
of the International Conference on Advances in Social Network Analysis and Mining 2009 (ASONAM'09). IEEE, 249–254.

[2] Lars Backstrom, Cynthia Dwork, and Jon Kleinberg. 2007. Wherefore art thou r3579x?: Anonymized social networks, hidden patterns, and structural steganography. In Proceedings of the 16th International Conference on the World Wide
Web (WWW'07)

[3] Ghazaleh Beigi, Kai Shu, Yanchao Zhang, and Huan Liu. 2018. Securing social media user data: An adversarial
approach. In Proceedings of the 29th Conference on Hypertext and Social Media. ACM, 165–173.

[4] Ghazaleh Beigi, Ruocheng Guo, Alexander Nou, Yanchao Zhang, and Huan Liu. 2019. Protecting user privacy: An approach for untraceable web browsing history and unambiguous user profiles. In Proceedings of the 12th ACM
International Conference on Web Search and Data Mining. ACM, 213–221.

[5] Ghazaleh Beigi. 2018. Social media and user privacy. Arxiv Preprint Arxiv:1806.09786 (2018).

[6] Ghazaleh Beigi and Huan Liu. 2019. Identifying novel privacy issues of online users on social media platforms by

Ghazaleh Beigi and Huan Liu, with Martin Vesely as coordinator. ACM SIGWEB Newsletter. Article 4 (Winter, 2019), 7
pages. http://doi.acm.org/10.1145/3293874.3293878

[7] Rui Li, Shengjie Wang, Hongbo Deng, Rui Wang, and Kevin Chen-Chuan Chang. 2012. Towards social user profileing: Unified and discriminative influence model for inferring home locations. In Proceedings of the ACM SIGKDD
Conference on Knowledge Discovery and Data Mining (SIGKDD'12).

[8] Ghazaleh Beigi, Suhas Ranganath, and Huan Liu. 2019. Signed link prediction with sparse data: The role of personality information. In Companion Proceedings of the Web Conference 2019. International World Wide Web Conferences
Steering Committee.

[9] Adrienne Porter Felt, Kate Greenwood, and David Wagner. 2011. The effectiveness of application permissions. In 2nd USENIX Conference on Web Application Development (WebApps 11).

[10] Asma Khatoon and Peter Corcoran. 2017. Android permission system and user privacy—a review of concept and approaches. In 2017 IEEE 7th International Conference on Consumer Electronics-Berlin (ICCE-Berlin). IEEE, 153–158.

[11] Primal Wijesekera, Arjun Baokar, Lynn Tsai, Joel Reardon, Serge Egelman, David
Wagner, and Konstantin Beznosov. 2017. The Feasibility of Dynamically Granted Permissions: Aligning Mobile Privacy with User Preferences. In 2017 IEEE Symposium on Security and Privacy (SP). 1077–1093. https://doi.org/10.1109/SP.2017.51

[12] Kavita Sharma and Brij B Gupta. 2019. Towards privacy risk analysis in android applications using machine learning approaches. International Journal of E-Services and Mobile Applications (IJESMA) 11, 2 (2019), 1–21.