# Privacy Policy Compliance in Miniapps: An Analytical Study

Yuyang Han
Beijing Electronic Science and Technology Institute
Beijing, China

Zilong Xiao
Beijing Electronic Science and Technology Institute
Beijing, China

Zhiqiang Wang
Beijing Electronic Science and Technology Institute
Beijing, China

Jianyi Zhang*
Beijing Electronic Science and Technology Institute
Beijing, China

## Abstract

Miniapps, lightweight applications based on WebView technology, are widely used on many platforms around the world. With the exponential growth in the number of miniapps, a variety of security concerns have emerged. Although various governments and miniapp vendors (platforms) have issued developer guidelines and privacy policies to address security issues, discrepancies between these policies across different countries and platforms can lead to ambiguous and inconsistent compliance. This inconsistency poses potential privacy risks for miniapp users. This paper aims to provide an innovative examination of the challenges and strategies relevant to ensuring compliance with miniapp privacy policies and regulations. We propose a compliance assessment framework to help developers navigate the complex legal landscape of privacy across multiple jurisdictions. Our goal is to enrich further the discourse surrounding the safe development of miniapps.

## CCS Concepts

• **Security and privacy → Social aspects of security and privacy**.

## Keywords

Miniapps, Security Risk, Privacy Policy, Security regulation

**ACM Reference Format:**
Yuyang Han, Zilong Xiao, Zhiqiang Wang, and Jianyi Zhang. 2024. Privacy Policy Compliance in Miniapps: An Analytical Study. In *Proceedings of the ACM Workshop on Secure and Trustworthy Superapps (SaTS '24), October 14–18, 2024, Salt Lake City, UT, USA.*. ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3689941.3695777

## 1 Introduction

In recent years, mobile super apps have gained significant momentum and made a significant impact in many areas. Super apps such as WeChat, Alipay, and TikTok provide users with comprehensive services through embedded miniapps. These miniapps, which can be used without downloading, have become increasingly popular on major platforms. While miniapps offer convenient services and a wide range of functionality, they also present security challenges, including vulnerabilities that can lead to user data breaches. These issues have heightened public concerns about user privacy and posed significant privacy challenges. In response to these challenges, various platforms have established specific guidelines for miniapp developers, regularly issued security patches, and enhanced functionalities to ensure robust protection of user privacy information.

At the same time, many countries and regions have progressively implemented a variety of user privacy and security policies aimed at regulating the collection, storage, processing and sharing of data. However, significant differences in policies across countries and platforms add layers of complexity and uncertainty to the global operation of miniapps. For example, regulations such as the General Data Protection Regulation (GDPR)[2] in the European Union and the California Consumer Privacy Act (CCPA)[3] in the United States impose strict requirements on data processing. Developers operating in multiple geographies must contend with multiple regulatory frameworks and compliance requirements. These differences can put miniapp users at risk, undermine user trust in platforms, and lead to legal and reputational consequences.

In this paper, we undertake a systematic exploration of the critical challenges and viable strategies that miniapps face in ensuring compliance with privacy policies and regulatory requirements. This study provides a comprehensive analysis of the similarities and differences in privacy policies across different countries and regions, highlighting the complexity of achieving global compliance. Specifically, we examine the following issues:

- `Global privacy regulatory environment`: An in-depth analysis of privacy law requirements in different jurisdictions, comparing the similarities and differences in privacy protections across countries.
- `Multi-platform compliance management`: An examination of how miniapps operating on different platforms (such as WeChat, Alipay, TikTok, etc.) can achieve consistency and compliance with privacy policies.
- `Privacy risks and user trust`: An analysis of potential privacy risks in cross-regional management and an exploration of technical and managerial approaches to enhance user trust.

To address these challenges, we propose a comprehensive compliance assessment framework. This framework is designed to guide developers through the complex landscape of privacy laws in different jurisdictions, providing systematic methods and insights

*Corresponding authors: zjy@besti.edu.cn


*SaTS '24, October 14–18, 2024, Salt Lake City, UT, USA.*

ACM ISBN 979-8-4007-1237-1/24/10
https://doi.org/10.1145/3689941.3695777

to facilitate more efficient privacy compliance management. The framework consists of the following components:

- `Legal analysis and guidance`: Provides in-depth analysis and compliance guidance on global privacy laws, helping developers understand and comply with privacy policies in different countries and regions.
- `Automated compliance assessment`: Leverages artificial intelligence and machine learning technologies to automatically assess and continuously monitor the privacy policies and data processing behaviors of miniapps.
- `Compliance updates and notifications`: Real-time monitoring of changes to privacy laws in different countries, timely updates to compliance policies, and distribution of compliance alerts and recommendations to developers.

By proposing and promoting this compliance assessment framework, we aim to help developers effectively address privacy challenges on a global scale, thereby promoting the safe development of the miniapp industry. We anticipate that our work will stimulate further industry discourse on privacy and compliance management and contribute to the creation of a safer, more transparent, and user-friendly miniapp ecosystem.

## 2 Background

### 2.1 Global privacy regulations

Global privacy regulations have had a profound impact on mobile application developers. Various countries and regions have enacted a series of stringent regulations aimed at protecting user privacy, which all companies that handle user data must comply.

In the European Union, the General Data Protection Regulation (GDPR) is one of the most stringent and influential privacy regulations in the world. The GDPR requires all data processing activities to be transparent and users to be informed about how their data is being used. Users have the right to access, correct, and delete their data and to restrict or object to data processing. The GDPR also sets out rules for cross-border data transfers and requires companies to promptly notify the relevant supervisory authorities and affected users in the event of a data breach.

In the United States, one of the most representative privacy laws is the California Consumer Privacy Act (CCPA). The CCPA provides California residents with broad privacy rights, including the rights of notice, access, deletion, and opt-out. The CCPA requires companies to obtain users' consent before selling their information and allows users to opt out of the sale of their information. The CCPA also requires that companies not discriminate against users who exercise their privacy rights.

In China, the Personal Information Protection Law (PIPL)[14] is the most recent central privacy regulation. It requires data processing to be lawful, fair, necessary, and limited to specific and clear purposes. The PIPL emphasises that the processing of personal information should be carried out with the informed consent of the user, who should be informed of the purpose, method, and scope of the processing. It imposes stricter requirements for the protection of sensitive personal information, such as biometric data. The PIPL also requires companies to establish and maintain robust data protection systems and take responsibility for compliance with their data processing activities.

The following table1 provides a comprehensive analysis of the similarities and differences between national and international privacy regulations. Our focus is on examining the differences between the privacy policies of the European Union, the United States, and China.

### 2.2 Compliance challenges

When deploying miniapps globally, developers face a myriad of compliance challenges. These challenges not only escalate compliance costs but also complicate management processes. The key challenges are

- `Multiple regulatory requirements`: Privacy regulations vary widely across jurisdictions, particularly in terms of data processing requirements and user rights protection. As a result, developers must tailor their data processing strategies to the specific regulatory framework of each region.
- `Regulatory conflicts and inconsistencies`: Data protection regulations enacted by different countries may contain conflicting or inconsistent provisions, particularly for data storage and transfer. These regulatory discrepancies require a high degree of legal acumen on the part of developers to mitigate the risk of non-compliance.
- `Evolving regulatory environment`: Data protection regulations are frequently updated and amended. Developers must remain vigilant and flexible to ensure that compliance measures are promptly adapted to meet new regulatory requirements.

### 2.3 Tools for miniapp development

The current market offers several tools and guidelines aimed at facilitating the development of miniapps. While these resources play an essential role in helping developers assess and comply with privacy regulations, they have some notable limitations due to the complexity of privacy and regional differences.

- `Insufficient functionality`: Some development tools lack full privacy compliance functionality and fail to provide comprehensive analysis and guidance on complex privacy regulations. As a result, developers must supplement these tools with legal advice and compliance experts, adding to development costs. For example, some tools may only provide basic privacy settings and identification capabilities but lack detailed monitoring of data processing activities and thorough compliance checks.
- `Limited coverage`: A significant number of existing tools are primarily tailored to the privacy regulations of specific regions (such as the EU or the US) and do not fully address the diverse global privacy requirements. This shortcoming forces developers to use multiple tools and manual methods when expanding internationally, increasing the management burden.

To overcome these challenges, more comprehensive and integrated tools are needed. These tools should include automated compliance assessments, real-time regulatory updates, and multi-jurisdictional coverage capabilities, enabling developers to efficiently and accurately comply with multiple privacy regulations. Our work echoes

**Table 1: Analysis of Similarities and Differences in Domestic and International Privacy Regulations**

| Regulation Clause | PIPL (China) | GDPR (EU) | CCPA (California) |
|---|---|---|---|
| Data Collection Consent | Explicit user consent required | Strict user consent required | Notification and consent required, but less stringent |
| User Control Rights | Users have the right to access and delete their data | Users have extensive rights to access, delete, correct, and transfer data | Users can request to know, delete, and opt-out of the sale of information |
| Data Minimization | Emphasizes data minimization | Strict enforcement of data minimization principle | Emphasizes transparency in data collection and use |
| Data Transfer | Supports cross-border transfer with security assurances | Strict regulations on cross-border data transfer, requiring equivalent protection levels | Emphasizes data security, but with less stringent specifics |
| Privacy Impact Assessment | Requires privacy impact assessments (PIPIA) in specific cases | Requires data protection impact assessments (DPIA) in most cases | No specific requirement, but emphasizes risk assessment in data processing |
| Data Breach Notification | Timely notification to users and authorities required | Data breaches must be reported to users and regulators within 72 hours | Timely notification to users required, but with less stringent timeframes |

such research trends in that we adopt a compliance-focused approach to address the identified challenges.

## 3 Methodology

### 3.1 Methodology overview

This section is the first time that the security issues of miniapps have been examined from the perspective of privacy policies and regulations. By synthesising the findings of miniapp analyses conducted in disparate geographical regions and across diverse technological platforms, we put forth a compliance assessment framework. The framework is capable of automatically identifying privacy policies within miniapps and comparing them with relevant regulations, thereby assisting developers in identifying potential compliance issues.

As illustrated in Figure 1, the framework comprises three modules, each of which plays a critical role in the process of data analysis and evaluation:

- `The Data Pre-training Module`: Comprehensive collection and preprocessing of data
- `The Database Construction Module`: Identify the optimal data storage mechanisms and dynamic updating processes
- `The Compliance analysis module`: Training of models, automated classification, and the analysis of detection

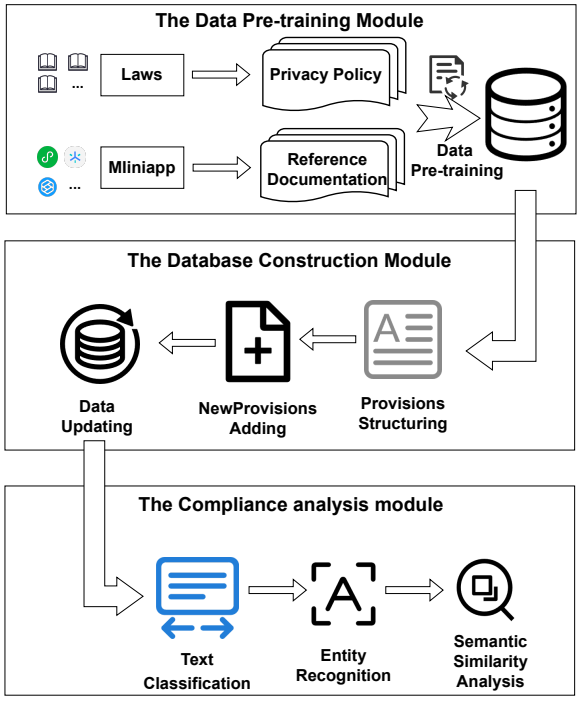


**Figure 1: Overview of Analyse Framework**

### 3.2 The Data Pre-training Module

The Data Pre-training Module serves as the foundational component of our framework, focusing on comprehensive data collection and preprocessing operations.

*3.2.1 Data Collection.* The data set consisted of the privacy policies of miniapps from a range of platforms, together with pertinent global privacy regulatory texts. The privacy policies for miniapps primarily encompass documentation content from developer tools on various platforms, including guides, frameworks, components, APIs, and additional sections. It is of particular relevance to consider the following global privacy regulations: The legislation under consideration includes China's "Personal Information Protection Law," "Cybersecurity Law[12]," and "Data Security Law"[13]; the United States CCPA (California Consumer Privacy Act) and CPRA (California Privacy Rights Act)[4]; and the GDPR (General Data Protection Regulation) and ePrivacy Directive[1]. To achieve the

objectives of this study, we selected three significant policies for detailed review, as shown in Table 1.

*3.2.2 Data Preprocessing.* The textual data collected was subjected to preprocessing to enhance the system's efficiency and accuracy, thus optimising the process. The following section presents an overview of the preprocessing steps.

Subsequently, the text was subjected to cleaning processes to ensure the accuracy and integrity of the data set. This work entailed the removal of any characters, HTML tags, or special symbols that were irrelevant to the subject matter, thus ensuring the data's relevance and coherence. The subsequent phase of the procedure entailed the processes of tokenization and annotation. Subsequently, the text was divided into discrete units, which were then subjected to part-of-speech tagging and named entity recognition. The stopword filtering process entailed the identification and removal of words that were deemed to be of little or no relevance within the context of the text being analysed. The elimination of words that are ubiquitous but devoid of particular significance.

## 3.3 The Database Construction Module

*3.3.1 Structuring Regulatory Provisions.* This study adopts the method of structuring the text of privacy regulations into a machine-readable format, aiming to improve the practicality and analysability of privacy regulations. This process involves the disaggregation of regulatory content into discrete provisions and sub-provisions, followed by the implementation of a systematic numbering and classification system. The primary sections are outlined as follows:

- `Provisions about data collection`: This section provides a comprehensive delineation of the parameters of personal data collection, establishes the legal justifications for such collection, and emphasises the principle of data minimisation. This work is done to guarantee that only the data required for the stated purposes is collected.
- `Provisions governing the utilisation of data`: This section imposes rigorous constraints on the utilisation of personal data, encompassing purpose limitation, data protection measures, and data retention durations, to prevent data misuse and ensure data security.
- `The Data Sharing Provisions`: This section provides detailed guidance on the circumstances under which data can be shared, including the user's right to be informed and the responsibilities of third parties. It ensures that user privacy is adequately protected during the data-sharing process.
- `The User Rights Provisions`: This section bestows upon users several rights about their data. These include the right of access, the right of correction, the right of deletion, and the right to port their data. The effect of these rights is to enable users to exercise control over their information and to make any necessary corrections or withdrawals.
- `Security provisions`: This section requires organisations to implement the necessary technical and managerial measures to ensure the security of data, prevent data breaches or losses, and promptly notify affected individuals and regulators in the event of a data breach.
- `Regulatory and Enforcement Provisions`: This section identifies the official bodies responsible for overseeing compliance with the data protection provisions and sets out the legal liabilities that may arise from breaches of these provisions.
- `International data transfer provisions`: This section sets out conditions and restrictions on the cross-border transfer of personal data and requires the signing of data protection agreements when international data transfers are involved.

*3.3.2 Regulatory update mechanism.* A regulatory update mechanism is designed to periodically obtain the latest privacy regulations from official sources and automatically update the database content, ensuring the timeliness and accuracy of the regulatory information.

- `Real-time collection`: Use web crawlers or official APIs (where available) to enable real-time download and capture of the latest regulatory documents.
- `Content verification`: Following the automated capture of regulatory content, pre-defined verification processes are applied to ensure the authenticity and accuracy of the information obtained, preventing the inclusion of incorrect or outdated data.
- `Database synchronization`: The verified regulatory content is synchronized with the database, incorporating revisions, additions, or repeals to existing regulations to maintain the completeness and up-to-dateness of the regulatory information within the database.

## 3.4 The Compliance analysis module

In order to improve the effectiveness of machine learning processing, we adopted the current mainstream pre-trained language model in this study. Transfer learning will be used to improve the model's performance in processing regulatory and privacy policy texts.

*3.4.1 Text classification.* A text classification model is developed to classify privacy policy texts into the above categories of legal provisions and to assess whether their content comprehensively covers all necessary legal requirements.

- `Data Input`: Pre-processed privacy policy texts
- `Data Output`: Classification labels and probabilities

*3.4.2 Named Entity Recognition (NER).* Named Entity Recognition (NER) technology is used to identify critical entities within privacy policies, such as data types, data collection methods, and data sharing parties, thereby ensuring the specificity and detail of policy content.

*3.4.3 Semantic similarity analysis.* Semantic similarity analysis is performed to assess the degree of alignment between the clauses in the privacy policies and the provisions in the regulatory database, thereby determining whether the policies comply with the regulatory requirements. This analysis uses techniques such as cosine similarity and BERT for semantic matching.

In addition, the compliance process includes the following:

- `Data collection and processing`: Review the developer guide's descriptions of data collection, processing, storage,

and sharing to ensure that they comply with the privacy policy.
- `User rights`: Evaluate the developer's guide descriptions of user rights to ensure compliance with the privacy policy.
- `Data security`: Evaluate the developer's guide descriptions of data security measures to ensure they are consistent with the privacy policy.
- `Third-party sharing`: Evaluate the developer's guide descriptions of data sharing with third parties to ensure both transparency and compliance with the user consent requirements of the privacy policy.

The evaluation process may reveal discrepancies between regulations in different countries and regions. For example:

- `Data protection laws`: The European Union's GDPR and China's PIPL have different data protection provisions. The GDPR emphasises the rights of data subjects and imposes restrictions on cross-border data transfers, while the PIPL imposes strict requirements on the processing of personal data.
- `User consent`: The requirements for user consent under the US CCPA and the Chinese PIPL differ. The CCPA requires companies to obtain explicit user consent when collecting and selling personal information, while the PIPL requires individual consent when processing sensitive personal data.

By following the steps and methodologies outlined above, it is possible to create an automated tool for assessing the compliance of miniapps, as well as analysing and addressing differences between different regulations. This approach can help developers ensure that their miniapps comply with relevant regulatory requirements, thereby reducing legal risks and protecting users' privacy.

# 4 Evaluation

## 4.1 Research Questions

We plan to conduct a large-scale evaluation of our framework, aiming at answering the following research questions (RQs):

- **RQ1 (Security): How can miniapps ensure compliance with the security requirements of different national privacy regulations when handling user data?**: This research question focuses our framework on examining and evaluating privacy regulations from other jurisdictions (such as the EU's GDPR and the US's CCPA) during the data collection process, as shown in Table1. By examining different national privacy regulations, our goal is to determine whether the security measures employed by miniapps are consistent with the privacy regulatory requirements of their respective target markets.
- **RQ2 (Consistency): How can we ensure that the privacy policies and practices of miniapps remain consistent across different platforms and different national privacy regulations?**: This research question requires that miniapps maintain consistent privacy policies and practices across platforms and countries to avoid user confusion or misunderstanding. In our study, we conducted consistency comparisons of developer documentation from different platforms, as shown in Table 33. Detailed analyses were performed on documents, APIs, and other components of developer documentation from five major miniapp platforms. We also analysed the similarities and differences in privacy policies across these different miniapp platforms, as shown in Table 22.
- **RQ3 (Compliance): How can the compliance of miniapps with global privacy regulations be assessed, and their ongoing compliance with evolving regulatory requirements be ensured?**: This research question addresses the compliance challenges faced by miniapps in the context of multiple privacy regulations. By using our framework to analyse data from miniapp developer documentation across platforms and reviewing rules from different countries, RQ3 aims to identify inconsistencies in the data. This study will also describe the characteristics of non-compliance. Previous research by our team has uncovered vulnerabilities such as CNVD-2024-05954, CNVD-2024-17193, and CNVD-2024-17868, all of which were caused by a lack of strict compliance with privacy regulations. Specifically, these vulnerabilities were caused by an inadequate configuration of permissions from the main program to the miniapps, resulting in significant breaches of user privacy.

## 4.2 Dataset Collection

When collecting regulations, we focus primarily on Chinese laws, such as the Data Security Law of the People's Republic of China, the Personal Information Protection Law of the People's Republic of China, and the Cybersecurity Law. For foreign privacy policies, we focus on relevant laws in the United States and the European Union, including the California Consumer Privacy Act (CCPA), the California Privacy Rights Act (CPRA), the Federal Trade Commission (FTC) 2023 Privacy and Data Security Update, the General Data Protection Regulation (GDPR), and the ePrivacy Directive. Specific regulations, such as the Personal Information Protection Law of the People's Republic of China, explicitly require all entities (including mobile applications) that process personal information to adhere to the principles of data minimisation, transparency, notice, and consent.

For the collection of developer documentation, our primary focus is on the privacy policies outlined in the developer documentation of various miniapp platforms. This study focuses on the five significant miniapps: WeChat, QQ, TikTok, Alipay, and Xiaohongshu. We collected and analysed their developer documentation related to privacy policies, including policies, frameworks, components, and APIs. Each platform's developer documentation provides a detailed overview of privacy policy rules, and the updated logs reveal the differences in privacy policy compliance among these miniapps.

# 5 Related work

In recent years, miniapps have emerged as a novel application paradigm that has attracted considerable academic interest. Research in this area can be categorised into two main areas.

**Table 2: Summary of Key Similarities and Differences in Privacy Policies Across Various Miniapp Platforms**

| Platform | User Data Collection Transparency | Data Minimization | User Consent Mechanism | User Rights | Data Protection Measures | Special Privacy Policies |
|---|---|---|---|---|---|---|
| WeChat MiniApps | Explicit | Strict | Mandatory | Access, Deletion, Correction | Mandatory Implementation | Protection of Minors |
| QQ MiniApps | Explicit | Moderate | Mandatory | Access, Deletion, Correction | Mandatory Implementation | Encrypted Data Transmission |
| TikTok MiniApps | Explicit | Moderate | Mandatory | Access, Deletion, Modification | Mandatory Implementation | UGC Privacy Protection |
| Alipay MiniApps | More Strict | Strict | Mandatory | Access, Deletion, Modification | Financial-grade Protection Measures | Financial Transaction Data Protection |
| Xiaohongshu MiniApps | Explicit | Moderate | Mandatory | Access, Deletion, Correction | Social Content Protection Measures | Social Interaction Data Protection |

**Table 3: Summary of Functionality Proportion and Analysis of Similarities and Differences in Privacy Policies Across Various Miniapp Platforms**

| Functionality Category | WeChat MiniApps | QQ MiniApps | TikTok MiniApps | Alipay MiniApps | Xiaohongshu MiniApps |
|---|---|---|---|---|---|
| Privacy Policy Display | 100% | 100% | 100% | 100% | 100% |
| User Data Collection | 100% | 90% | 100% | 100% | 100% |
| User Data Storage | 100% | 90% | 100% | 90% | 100% |
| Data Usage Explanation | 100% | 100% | 100% | 100% | 95% |
| Data Sharing Terms | 95% | 90% | 95% | 90% | 90% |
| User Rights Terms | 100% | 100% | 100% | 100% | 100% |

## 5.1 MiniApp privacy

Several previous studies have highlighted the importance of privacy in miniapps[5, 7, 8, 11, 15, 20, 21]. MINITAINTDEV[17] proposed a dynamic taint analysis engine. TaintMini[9] introduced a framework for detecting sensitive data flows within and between miniapps using static taint analysis. Wang and colleagues proposed a two-step hybrid analysis method, MiniScope, which integrates dynamic UI exploration to identify privacy inconsistencies in miniapps pragmatically. In addition, studies such as [5, 8, 21] have focused on taint analysis techniques to detect application data leaks. Notably, another work[11] concentrates on the consistency of data collection and usage within miniapps.

## 5.2 MiniApp security

Recent studies have investigated the security concerns of miniapps and have uncovered many vulnerabilities and threats[6, 10, 18, 19, 22]. Wang et al. [9] developed a mechanism called TaintMini to monitor tainted data flows within miniapps. Yang et al. [16] developed the Cmrf scanner to detect the lack of application checks in cross-miniapp requests. In addition, [19] investigated a novel issue related to privacy leaks in miniapps, which could potentially lead to the unauthorized acquisition of private data by miniapp platforms.

# 6 Conclusion

This study pioneers the public examination of privacy policies in miniapps, highlighting an area that has emerged as a critical focus within the field of miniapp security. To address this, we present a compliance framework that aims to assist developers in understanding and to comply with the privacy policies and regulatory requirements of miniapps within mobile super-applications. This framework consists of three essential modules that represent a novel methodology for investigating the privacy and security of miniapps. Future research will further explore issues related to compliance, scalability, and privacy consistency. Our research represents the first focused analysis of privacy policies in the area of miniapp security. This pioneering work contributes to the overall advancement of the field of mobile application security.

# Acknowledgments

Supported by the Shenyang Science and Technology Plan (22322335).

# References

[1] 2002. ePrivacy Directive. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32002L0058
[2] 2018. General Data Protection Regulation. https://gdpr-info.eu/
[3] 2020. California Consumer Privacy Act. https://oag.ca.gov/privacy/ccpa
[4] 2023. California Privacy Rights Act(CPRA). https://www.caprivacy.org/
[5] Supraja Baskaran, Lianying Zhao, Mohammad Mannan, and Amr Youssef. 2023. Measuring the leakage and exploitability of authentication secrets in super-apps:

The wechat case. In *Proceedings of the 26th International Symposium on Research in Attacks, Intrusions and Defenses*. 727–743.

[6] Yuyang Han, Xu Ji, Zhiqiang Wang, and Jianyi Zhang. 2023. Systematic Analysis of Security and Vulnerabilities in Miniapps *(SaTS '23)*. Association for Computing Machinery, New York, NY, USA, 1–9. https://doi.org/10.1145/3605762.3624432

[7] Wei Li, Borui Yang, Hangyu Ye, Liyao Xiang, Qingxiao Tao, Xinbing Wang, and Chenghu Zhou. 2023. Minitracker: Large-scale sensitive information tracking in mini apps. *IEEE Transactions on Dependable and Secure Computing* (2023).

[8] Shi Meng, Liu Wang, Shenao Wang, Kailong Wang, Xusheng Xiao, Guangdong Bai, and Haoyu Wang. 2023. WeMinT: Tainting Sensitive Data Leaks in WeChat Mini-Programs. In *2023 38th IEEE/ACM International Conference on Automated Software Engineering (ASE)*. IEEE, 1403–1415.

[9] Chao Wang, Ronny Ko, Yue Zhang, Yuqing Yang, and Zhiqiang Lin. 2023. Taintmini: Detecting Flow of Sensitive Data in Mini-Programs with Static Taint Analysis. In *2023 IEEE/ACM 45th International Conference on Software Engineering (ICSE)*. 932–944. https://doi.org/10.1109/ICSE48619.2023.00086

[10] Chao Wang, Yue Zhang, and Zhiqiang Lin. 2023. Uncovering and Exploiting Hidden APIs in Mobile Super Apps. arXiv:2306.08134 [cs.CR]

[11] Yin Wang, Ming Fan, Junfeng Liu, Junjie Tao, Wuxia Jin, Qi Xiong, Yuhao Liu, Qinghua Zheng, and Ting Liu. 2023. Do as you say: Consistency detection of data practice in program code and privacy policy in mini-app. *arXiv preprint arXiv:2302.13860* (2023).

[12] XinHua. 2016. Data Security Law. https://www.gov.cn/xinwen/2016-11/07/content_5129723.htm

[13] XinHua. 2021. Cybersecurity Law. https://www.gov.cn/xinwen/2021-06/11/content_5616919.htm

[14] XinHua. 2021. The Personal Information Protection Law (PIPL). https://www.gov.cn/xinwen/2021-08/20/content_5632486.htm

[15] Yuqing Yang, Chao Wang, Yue Zhang, and Zhiqiang Lin. 2023. Sok: Decoding the super app enigma: The security mechanisms, threats, and trade-offs in os-alike apps. *arXiv preprint arXiv:2306.07495* (2023).

[16] Yuqing Yang, Yue Zhang, and Zhiqiang Lin. 2022. Cross miniapp request forgery: Root causes, attacks, and vulnerability detection. In *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*. 3079–3092.

[17] Jianjia Yu, Zifeng Kang, and Yinzhi Cao. 2023. MiniTaintDev: Unveiling Mini-App Vulnerabilities through Dynamic Taint Analysis. In *Proceedings of the 2023 ACM Workshop on Secure and Trustworthy Superapps*. New York, NY, USA, 41–45. https://doi.org/10.1145/3605762.3624434

[18] Jianyi Zhang, Leixin Yang, Yuyang Han, Zixiao Xiang, and Xiali Hei. 2023. A small leak will sink many ships: Vulnerabilities related to mini-programs permissions. In *2023 IEEE 47th Annual Computers, Software, and Applications Conference (COMPSAC)*. IEEE, 595–606.

[19] Lei Zhang, Zhibo Zhang, Ancong Liu, Yinzhi Cao, Xiaohan Zhang, Yanjun Chen, Yuan Zhang, Guangliang Yang, and Min Yang. 2022. Identity Confusion in WebView-based Mobile App-in-app Ecosystems. In *31st USENIX Security Symposium (USENIX Security 22)*. USENIX Association, Boston, MA, 1597–1613. https://www.usenix.org/conference/usenixsecurity22/presentation/zhang-lei

[20] Xiaohan Zhang, Yang Wang, Xin Zhang, Ziqi Huang, Lei Zhang, and Min Yang. 2023. Understanding Privacy Over-collection in WeChat Sub-app Ecosystem. *arXiv preprint arXiv:2306.08391* (2023).

[21] Yue Zhang, Yuqing Yang, and Zhiqiang Lin. 2023. Don't leak your keys: Understanding, measuring, and exploiting the appsecret leaks in mini-programs. In *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security*. 2411–2425.

[22] Zhibo Zhang, Lei Zhang, Guangliang Yang, Yanjun Chen, Jiahao Xu, and Min Yang. 2024. The Dark Forest: Understanding Security Risks of Cross-Party Delegated Resources in Mobile App-in-App Ecosystems. *IEEE Transactions on Information Forensics and Security* 19 (2024), 5434–5448. https://doi.org/10.1109/TIFS.2024.3390553