Privacy Law Enforcement Under Centralized Governance: A Qualitative Analysis of Four Years' Special Privacy Rectification Campaigns

Tao Jing[1,2,*], Yao Li[3], Jingzhou Ye[3], Jie Wang[1,2,✉,*], and Xueqiang Wang[3]

[1] *School of Cyber Science and Engineering, Huazhong University of Science and Technology*
[2] *JinYinHu Laboratory*
[3] *University of Central Florida*
✉ *Corresponding author: wangjie_s@hust.edu.cn*

Abstract

In recent years, major privacy laws like the GDPR have brought about positive changes. However, challenges remain in enforcing the laws, particularly due to under-resourced regulators facing a large number of potential privacy-violating software applications (apps) and the high costs of investigating them. Since 2019, China has launched a series of privacy enforcement campaigns known as Special Privacy Rectification Campaigns (SPRCs) to address widespread privacy violations in its mobile application (app) ecosystem. Unlike the enforcement of the GDPR, SPRCs are characterized by large-scale privacy reviews and strict sanctions, under the strong control of central authorities. In SPRCs, central government authorities issue administrative orders to mobilize various resources for market-wide privacy reviews of mobile apps. They enforce strict sanctions by requiring privacy-violating apps to rectify issues within a short timeframe or face removal from app stores. While there are a few reports on SPRCs, the effectiveness and potential problems of this campaign-style privacy enforcement approach remain unclear to the community.

In this study, we conducted 18 semi-structured interviews with app-related engineers involved in SPRCs to better understand the campaign-style privacy enforcement. Based on the interviews, we reported our findings on a variety of aspects of SPRCs, such as the processes that app engineers regularly follow to achieve privacy compliance in SPRCs, the challenges they encounter, the solutions they adopt to address these challenges, and the impacts of SPRCs, etc. We found that app engineers face a series of challenges in achieving privacy compliance in their apps. For example, they receive inconsistent app privacy review reports from multiple app stores and have difficulties confirming the issues flagged by these reports; they also lack institutional support for studying privacy laws, self-validating privacy compliance of their apps, communicating effectively between multiple stakeholders, and ensuring fairness in accountability when privacy non-compliance occurs. Furthermore, we found that while SPRCs have introduced several positive changes, there remain unaddressed concerns, such as the potential existence of circumvention techniques used to evade app privacy reviews.

1 Introduction

"Laws without enforcement are just good advice."

- Abraham Lincoln

Recent studies have shown that the enforcement of privacy laws has led to a variety of positive changes, such as improved privacy policies [40, 81], reduced use of tracking cookies [39], and even increased company revenues [17]. However, challenges still exist in enforcing the laws, particularly due to under-resourced regulators [25] and the high costs of investigating privacy-violating software applications (apps). For example, the Federal Trade Commission (FTC), which enforces the Children's Online Privacy Protection Act (COPPA) [18], takes an average of 294 days to complete an investigation [20], a lengthy process that includes evidence collection, violation assessment, and court proceedings, etc. Considering the large number of apps available (in the millions on mobile platforms [63]), many apps may not undergo external privacy reviews, even though they pose privacy risks [35, 56].

Since October 2019, China has launched a series of privacy enforcement campaigns known as the Special Privacy Rectification Campaigns (SPRCs) [42–45] to tackle the widespread privacy violations in its mobile app ecosystem. Unlike the lengthy investigation process, SPRCs are characterized by large-scale and strict sanctions for privacy governance, under the strong control of central authorities such as the Ministry of Industry and Information Technology (MIIT) [41]. These authorities issue administrative orders that specify detailed privacy compliance requirements, and mobilize necessary resources (including major app stores and third-party privacy certifiers) to conduct comprehensive, market-wide privacy reviews of mobile apps. Apps found to have privacy violations must be rectified by their providers within a defined timeframe (e.g., five business days), or the apps risk being listed

*Hubei Key Laboratory of Distributed System Security, Hubei Engineering Research Center on Big Data Security, School of Cyber Science and Engineering, Huazhong University of Science and Technology.

on public privacy bulletins by the MIIT or removed from app stores [42–45]. According to available data as of June 2022, MIIT has conducted intensive privacy reviews for over 3.22 million apps, resulting in the removal of at least 3,000 apps from app stores [60].

However, although there are a few government reports on SPRCs [60, 66], the effectiveness and potential problems of such a campaign-style enforcement approach, characterized by large-scale privacy reviews and strict sanctions, remain largely unknown to both industry and academia. Understanding this approach is crucial not only for evaluating the outcomes of China's investment in privacy law compliance but also for guiding future steps in this area. Moreover, in the long term, analyzing this campaign-style enforcement approach can provide valuable insights into alternative methods of privacy law enforcement and potentially improve privacy compliance efforts in other countries.

This study qualitatively analyzes SPRCs to better understand the effectiveness and potential problems in these large-scale enforcement efforts. Specifically, we plan to answer the following research questions:

RQ1: What is the workflow that privacy stakeholders regularly follow in SPRC?

RQ2: What challenges did app developers encounter in achieving app privacy compliance in SPRCs?

RQ3: What solutions have the app developers adopted to address these challenges?

RQ4: What are the overall impacts of the SPRCs?

To answer these questions, we conducted a semi-structured interview study involving 18 app-related engineers who have been involved in SPRCs. These participants consist of app developers, technical leads, security engineers, and test engineers, all of whom have experience in ensuring privacy compliance with SPRCs for mobile apps. Based on these interviews, we report the following key insights:

- *Inconsistencies manifest in a variety of aspects of SPRCs.* For instance, an app may receive different privacy review reports from multiple app stores, and these reports can also be different to the developers self-test results, which cause frustration for app developers. Also, app stores have differing definitions of sensitive data with app developers, and they treat popular apps more strictly than unpopular apps during app review.

- *There is a lack of institutional support from the app providers for privacy compliance.* App developers reported that, to achieve privacy compliance, they need more support for studying privacy laws, more resources to self-validate privacy compliance, more support for communication, and fairness in accountability.

- *SPRCs result in both positive changes and concerns regarding privacy compliance.* Overall, participants reported that SPRCs reduced the number of privacy-invading apps and increased awareness of the significance of privacy among app engineers. However, they expressed particular concern about the existence of circumvention techniques used to evade app privacy reviews.

2 Background

2.1 Enforcement of EU and US Privacy Laws

The General Data Protection Regulation (GDPR) [3], which came into effect on May 25, 2018, is a comprehensive legal framework designed to protect the privacy rights of individuals in the European Union (EU). To enforce the GDPR, Data Protection Authorities (DPAs) in each EU member state undertake various tasks to monitor organizational compliance, investigate potential violations, promoting public awareness, etc. The investigation process, in particular, can be time-consuming [50] due to the need for comprehensive data reviews, legal assessments, and the detailed procedural steps required for potential court proceedings. Privacy legislation in the US is based on both federal and state privacy laws. The enforcement of each privacy law is similar to the GDPR in that it relies on enforcement actions by federal or state supervisory agencies, under the guidance of privacy laws. Examples are the Children's Online Privacy Protection Act (COPPA) [18], enforced by the Federal Trade Commission (FTC) [19], and the California Consumer Privacy Act (CCPA) [22], enforced by the California Attorney General's office [21].

2.2 Enforcement of Chinese Privacy Laws

Unlike the enforcement of GDPR and US privacy laws, China adopts a different approach by enforcing its privacy laws through nationwide campaigns, similar to how it enforces other laws [73, 75–77, 79, 82, 84]. In recent years, Chinese government agencies have launched several privacy enforcement campaigns to conduct large-scale privacy reviews of mobile apps, imposing strict sanctions based on various privacy laws, provisions, and guidelines.

Chinese privacy laws, provisions, and guidelines. There are several Chinese privacy laws that outline general privacy principles in a manner similar to GDPR, such as the Cybersecurity Law (2016) [14], the Regulations on Telecommunications (2000) [51], and the Personal Information Protection Law (PIPL, 2021) [52], etc. Based on these laws, Chinese government agencies, such as the Ministry of Industry and Information Technology (MIIT), issue provisions to address specific details of the general privacy principles. For example, the "Provisions on Protecting the Personal Information of Telecommunications and Internet Users" (MIIT Order No. 24, 2013) [15] and the "Provisions on the Scope of Necessary Personal Information for Common Types of Mobile Applications" (CAC Order No. 14, 2021) [16] specify requirements for

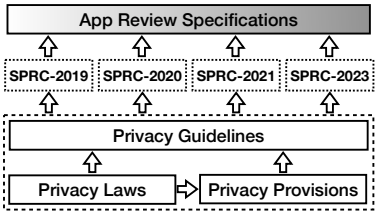


Figure 1: Hierarchy of privacy laws, provisions, guidelines, and app review specifications

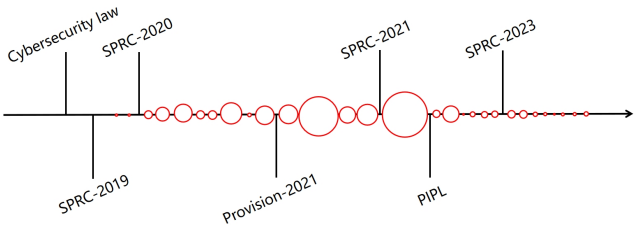


Figure 2: Timeline of SPRCs and privacy bulletins issued by government agencies. Each circle (◯) represents a bulletin, with the size of the circle indicating the number of reported apps with privacy violations.

protecting the personal information and rights of Internet users, including mobile app users. Besides the privacy laws and provisions, government agencies can also release privacy guidelines that offer more practical guidance on interpreting or implementing laws and provisions. For example, on December 30, 2019, MIIT issued a privacy guideline in MIIT Secret [2019] No. 191, titled "Means for Determination of Violations of Laws and Regulations in Apps' Collection and Use of Personal Information" (*Guideline-2019*) [46]. Although the guideline is not legally binding, it has evolved into a de facto standard used by stakeholders to assess privacy violations in apps. Figure 1 shows the relationship between privacy laws, provisions, and guidelines.

Special Privacy Rectification Campaigns (SPRCs). While agencies like MIIT also support community-based efforts such as responding to individual complaints and public reports, their predominant enforcement efforts so far have focused on launching nationwide privacy campaigns, often referred to as *Special Privacy Rectification Campaigns* (SPRCs). Specific to the enforcement on mobile platforms, MIIT, in collaboration with three other government agencies including the Cyberspace Administration of China (CAC), has initiated four SPRCs that have spanned over four years. In October 2019, MIIT launched an SPRC (*SPRC-2019* [45]) by issuing an administrative notice to stakeholders aimed at rectifying mobile apps' infringement of users' privacy rights and interests. Later, in August 2020, July 2021, and February 2023, MIIT revitalized the program with another three SPRCs, *SPRC-2020* [44], *SPRC-2021* [43], and *SPRC-2023* [42], respectively, to further enhance the objectives set forth in prior SPRCs. Note that the newer SPRCs do not disable but rather complement prior SPRCs by addressing a broader scope of problems or by prioritizing the types of privacy violations that warrant more attention. For example, SPRC-2019 requires that app developers and distribution platforms (i.e., app stores) detect and rectify eight types of privacy violations related to the collection, use, and sharing of personal information, as well as the ease of deleting user accounts. SPRC-2020 also covers these violations and expands the requirements to include emerging violations, such as in personalized ads and deceptive privacy practices, and involves new stakeholders, such as third-party SDK developers.

According to administrative notices [42–45], the SPRCs conduct two types of app privacy reviews: government agencies perform privacy reviews on existing apps in app stores, either directly or via third-party privacy certification services (certifiers), and major app stores are required to conduct privacy reviews for newly submitted apps. Typically, privacy certifiers and app stores develop their own sets of app review specifications based on the administrative notices of SPRCs. If an app is found to have privacy violations, the app provider must rectify them; otherwise, there is a risk of the app being delisted or facing fines. Notably, the SPRCs are not short-term campaigns but represent long-term, ongoing efforts that have extended for more than four years until now. To date, the agencies have issued warnings of delisting through 36 public privacy bulletins on their websites (such as [47]), akin to walls of shame, with each bulletin listing hundreds (or at least dozens) of privacy-violating apps. Figure 2 shows the SPRCs and release time of the privacy bulletins.

3 Methodology

In fall 2023, we conducted a semi-structured interview study with 18 participants who have been involved in the privacy compliance with SPRCs, to explore their experience and perception of China's large-scale SPRCs, as well as their challenges and solutions.

3.1 Recruitment of Participants

We adopted convenience sampling to recruit participants who have been involved in SPRCs on WeChat [67] – one of the largest social media in China. Through our personal networks, we joined five WeChat groups with names such as "App Privacy Compliance Discussion Group". These groups are composed of a total of 1,600 members who have worked on privacy compliance from different industries and companies. The group members discuss a variety of privacy compliance issues, such as how to use the detection tools, how to address noncompliance, and what is the latest reported noncompliance and the updated privacy review specifications. To reach a more diverse sample, we were then referred to another four groups by our participants. However, after reviewing the chat history for one week, there was no privacy compliance-related content found in the these four groups, and thus we did not recruit from these groups. We posted recruitment information in the WeChat groups, in which we described the purpose and procedure of

the interview study, as well as eligibility and compensation. We also used snowball sampling [26] by asking interviewees to share our recruitment information with their friends and colleagues, who might be interested in privacy research.

Eligible interviewees are those who are above 18 years old and had at least one year's experience in privacy compliance. Besides eligibility, we also considered the diversity of the interviewees. The recruited interviewees take different roles in privacy compliance in their companies, such as app developers, technical lead, app testers, and security engineers. The apps they work on included finance, gaming, and education. Additionally, interviewees' companies were located in different cities in China, with company sizes ranging from 20 to 200,000 employees. In total, we interviewed 18 participants, who spread across 10 different cities, with various roles and responsibilities in privacy compliance. We observed thematic saturation after coding 16 interviews, when no new codes were created. Therefore, we stopped interviewing new participants after 18 interviews and believe that we reached theoretical saturation. Of the 18 participants, 15 were recruited through convenience sampling and 3 through snowball sampling. Notably, one interviewee was in Singapore, who had developed an e-commerce app for users in China, listed in Chinese app stores. We included this interviewee because they also had experience with privacy compliance in China. Interviewees' information is listed in Table 1. We offered 100 RMB to each interviewee. The study was approved by IRB and followed the procedures of the Ethics Review Committee.

3.2 Interview Process

We informed the interviewees about the purpose and procedures of this study and collected their consent before the interview. The interviews were conducted in Mandarin using WeChat call, lasting between 50-70 minutes. Interviews was audio recorded for transcription, with interviewees' consent.

We first asked general questions about interviewees' industry, company size, job duties, and other background information, to collect some contextual information about their work in privacy compliance. Next, we probed their knowledge about privacy compliance in China, by asking them when, how, what and why they had learned about the privacy laws, provisions, guidelines and procedures released by the government. Based on their familiarity with privacy compliance, we probed into how they understand, interpret and perceive the privacy compliance in the development of apps, as well as how they achieve privacy compliance, such as the methods, tools, and strategies they have used. Particularly, we asked about the steps they needed to go through to have their apps reviewed by app stores and governmental agencies. We probed into the challenges, problems, and difficulties they encountered during the review. We also encouraged them to share their opinions, feelings and strategies about the review. All the translated interview questions can be found in https://github.com/YkGUWbrF/SPRC.

3.3 Interview Analysis

We used inductive thematic analysis [12] to analyze the interviews. We first transcribed the audio-recorded interviews into text and anonymized interviewees' identifiable information. Once the transcription was done, we deleted the audio recordings to protect interviewees' privacy. Next, we read all the transcribed interviews, familiarized ourselves with the data, and independently noted down the initial codes related to interviewees' understandings, perceptions, practices, challenges and strategies in privacy compliance. These codes are meaningful labels attached to specific segments of the interview data. Then, we compared our initial codes with each other, went back and forth between codes and original data, discussed our interpretations about each individual code, and revised/refined the codes through multiple meetings. This step ended with compiling a comprehensive list of 875 codes. Based on the initial codes, we collated similar codes into a sub-theme, which identified 22 sub-themes. We first gathered all the original data relevant to each sub-theme, examined the codes and associated data, examined the relationships between the codes, and collapsing similar codes into a bigger and meaningful pattern. Then we further grouped similar sub-themes into an overarching theme by identifying the relationships between the sub-themes. We identified 4 overarching themes, namely privacy review workflow, challenges to app developers, solutions to address challenges, and positive changes and concerns. A thematic map was thus formed, with 4 themes, 22 sub-themes and 875 codes. With the initial thematic map developed, we reviewed and refined it by checking whether the themes/subthemes captured the meanings in the coded data segments and formed a coherent pattern.

4 Results

4.1 RQ1: Privacy Review Workflow

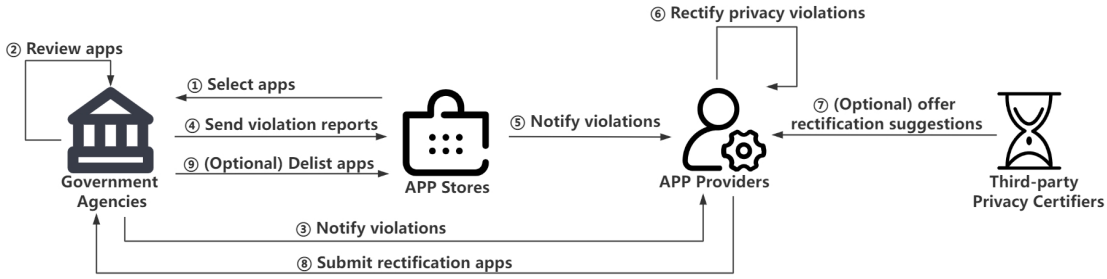
Based on the interviews, we summarize a workflow that participants regularly go through in privacy reviews. We first introduce the stakeholders in the workflow, and then report the procedures in the SPRC privacy review and app store privacy review, as two fundamental components in the workflow.

4.1.1 Stakeholders

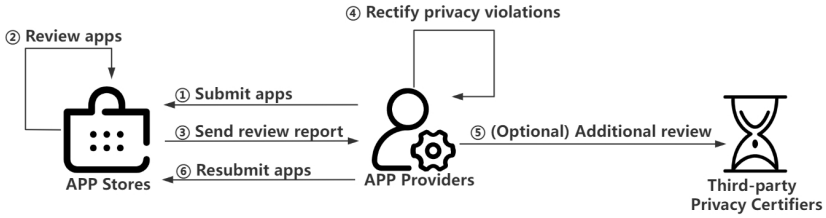
As mentioned in Section 2.2, the enforcement of Chinese privacy laws on mobile apps has primarily been driven by large-scale campaigns, i.e., SPRCs, and involves multiple stakeholders. In the following, we highlight the major stakeholders identified by our interviewees, and we will refer to these stakeholders throughout the paper.

• **App providers** refer to the companies where the interviewees are employed. If privacy violations are detected in their apps during the reviews, app providers, such as the companies of P6, P8 and P12, will be notified by the government or the app stores.

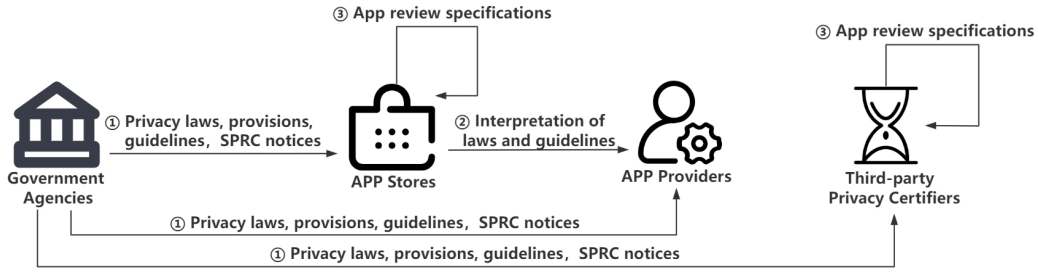
• **App engineers** are employees hired by app providers who conduct the technical design, development, and testing of



(a) SPRC privacy review workflow



(b) App store privacy review workflow



(c) Information flow

Figure 3: Privacy Enforcement Workflows

mobile apps. Most of our interviewees are in this role.

• **App users** are the individuals from whom mobile apps collect personal data. In this study, interviewees also referred to app users as "end users", "individuals", or "clients".

• **App stores** are the marketplaces where app users can find and download apps. Interviewees interacted with several app stores in China, such as OPPO, Huawei, and Apple Store, for app store privacy review (detailed in 5.1.2) .

• **Third-party privacy certifiers** emerge due to the increasing concerns and challenges in privacy reviews. Interviewees reported that they submitted their apps to these certifiers, such as Bangcle Security [59] and iJiami [30], for additional privacy review, with the aim to prevent potential privacy violations. Their companies needed to pay the certifiers every time their apps are reviewed.

• **Government agencies** are executive departments of China, including MIIT and CAC, along with their affiliated institutions such as CAICT (China Academy of Information and Communications Technology). We use government agencies to represent all of them. Interviewees noted that these government agencies are responsible for issuing privacy laws, provisions, and guidelines, and issuing administrative notices to launch SPRCs (detailed in 5.1.2).

4.1.2 Privacy Enforcement Workflows

Interviewees reported that mobile apps need to go through two types of privacy review:

SPRC privacy review workflow. As shown in Figure 3a, interviewees explained that the SPRC privacy review is initiated by government agencies to select a subset of apps available in major app stores (①). This review is periodical, occurring every 1-2 month. The selected subset of apps usually favors those with a large user base in China. Government agencies either collaborate with third-party privacy certifiers or build their own certification services, to conduct this periodical privacy review (②). For instance, P3 and P8 told us:

"From what I know, the MIIT has entrusted the CAICT to build their own [app privacy review] platform."

"The MIIT also invites some third-party privacy certifiers."

If an app is found to have privacy violations, the government agencies will issue a public bulletin regarding the app's pri-

vacy violations on government websites (③). Subsequently, the government agencies will send the app review reports containing the violations to the app stores (④). App providers are then notified of the privacy violations of their apps and receive the reports from the app stores (⑤). The app providers need to address the privacy violations based on the reports (⑥). If the app providers have purchased the service from the third-party privacy certifiers, the third-party certifiers will provide compliance services and rectification suggestions to app providers based on violation reports (⑦) It's important to note that, due to the presence of privacy violations, app providers are only given a short period of time, typically 5 business days, to rectify their apps. Once the app providers address the violations in a new version, they will submit it to the government agencies for a second review (⑧). If the new version fails to address the violations adequately, government agencies will notify app stores to remove the apps from their listings (⑨). For example, P3 noted:

"They [government agencies] implemented two mechanisms, notification [placing on bulletins] and app store removal. If the rectification is not completed within five days, then the app is removed from the app stores."

App store privacy review workflow. As shown in Figure 3b, the interviewees reported that once an app is developed, its provider submits it to app stores for privacy review before making it available for end users (①). The app stores review the app in accordance with their app review specifications (②), which are drafted based on the privacy laws, provisions and guidelines from the government agencies. If no privacy violations are identified during the review process, the app will be published in the app stores without any changes. However, if privacy violations are detected, the app stores will generate a privacy review report and send it to the app provider (③). The app provider must address the violations in the review reports (⑥). It's worth noting that this rectification and resubmission process may occur multiple times until all violations are appropriately resolved. For app providers are concerned with potential privacy noncompliance, they may choose to conduct an internal privacy review on their own (④) or pay third-party privacy certifiers for pre-review (⑤), before submitting to app stores. These reviews (④ and ⑤) are optional and can take place in any sequence. For instance, P9 shared:

"We need to publish our apps on five different app stores, Xiaomi, Huawei, and then Vivo, and AppGallery. When you submit your app, there are usually one or two app stores that don't pass the review, and then you have to revise."

Information flow. In addition to the aforementioned workflows, interviewees also mentioned an information flow stemming from privacy laws (as depicted in Figure 3c). Specifically, app providers, app stores, and third-party certifiers take the privacy laws, provisions, and guidelines issued by government agencies as input (①). Subsequently, app providers strive to develop privacy-compliant apps based on their interpretation of the laws, provisions and guidelines (②). App stores and third-party certifiers build their app review specifications in line with the administrative notices of SPRCs, based on privacy laws, provisions, and guidelines. Interviewees, such as P5 and P18, indicated that the app review specifications would update frequently with the updates of SPRCs (③).

Interviewees report that SPRCs involve various stakeholders such as app providers, app stores, third-party privacy certifiers, and government agencies. In SPRCs, mobile apps undergo two types of privacy reviews: the SPRC privacy review and the app store privacy review.

4.2 RQ2: Challenges to App Developers

We report three major challenges that interviewees have encountered in the privacy reviews and privacy compliance.

4.2.1 Inconsistencies

Same app receives inconsistent privacy review reports from different app stores. Eight interviewees (from both small companies, such as those of P7 and P9, and relatively large companies with over 1,000 employees, such as those of P1, P8, P14, P16, P17, and P18) mentioned that they received privacy review reports with inconsistent results when submitting their apps to multiple app stores for review. Each app store develops their own privacy review specifications and tools based on the laws, provisions and guidelines issued by the government. They may interpret and implement the laws differently. The interviewees attributed the inconsistency of the results to the different detection tools adopted by the app stores, as app stores do not always update their tools at the same time. They also do not implement all the updates at once, but selectively deploy important updates that they value first. P9 pointed out that some app stores, citing Xiaomi as an example, even outsource their privacy reviews to different third-party privacy certifiers, each providing different services or offerings. These issues led to privacy violations reported by one app store but not by the other. As a result, app developers need to invest a large amount of time to triage the reports from the app stores and explore the reasons behind the inconsistent detection results, which wastes their time that were supposed to be spent on privacy violation mitigation. For example, P9 noted:

"Those app stores often outsource their privacy vetting to over ten different third-party companies, and therefore, the results sometimes are not consistent."

In addition to the inconsistent app review results from app stores, the quality of the app stores' reports, such as the granularity and comprehensiveness of results, also varies between app stores. Participants reported that some app stores, such as OPPO and Vivo, present detailed information about privacy violations in their reports, including class/method names and app stack traces, making it easy for app developers to pinpoint the exact reason behind the violations. However, other app stores, such as Xiao Mi, failed to provide these

details. They simply listed the general privacy violations without why and where, leaving the developers to explore on their own. Such exploration demands significant effort from developers, since searching for the causes (e.g., piece of code) of the violations and confirming them can be tedious and time-consuming. It becomes even more difficult considering that the code that leads to the violations may not be developed by their own teams, and in many cases, not even from the same company (e.g., third-party code). For example, P4 told us:

"For instance, from my perspective, OPPO and vivo provide similar reports in an Excel spreadsheet, detailing stack information. In contrast, platforms like Xiaomi and Yingyongbao don't provide such details, just a table, very general about the problems, leaving you to investigate yourself. This can be rather troublesome."

App developers' self-testing results are different from app stores' privacy review reports. The privacy violations identified by app stores often do not show up when app developers test their apps themselves. Two interviewees (P7, P14) noted that app stores reported violations in their apps for collecting sensitive data and for posting permission requests before users accept privacy policies. But these violations could only be found in the devices used by the app stores. When the app developers tested the apps on their own devices, they had a difficult and frustrating time reproducing the reported violations because they were unable to observe the behaviors in the apps. The major cause of this issue is that the app stores used different devices to test the apps from the app developers, and the app violating behaviors show up only on those devices. For example, P7's app turned out to collect additional data on app store's device (Huawei Mate 50 series devices). P14's app tended to post additional permission requests before privacy policies on app store's device. But these issues did not show up in app developer's devices. It is impractical to ask app developers to adopt the same devices as the app stores', because they are unaware of the devices that the app stores would use, among hundreds of different existing devices, before the review. For instance, P7 said:

"The device model, which can sometimes lead to different test results... testing on the Huawei Mate 50 series (in app store review), an app was found to collect data... However, this issue was not observed in other device models."

App developers and app stores define sensitive personal data differently. App developers and app stores often have an inconsistent understanding of what personal data should be considered sensitive and warrant better protection through the enforcement of privacy laws. This inconsistency mainly concerns user-specific and device-specific data. Particularly, P9 believes that data directly associated with users (e.g., phone number, family information) is highly sensitive, while device-specific data alone (e.g., Android ID, IMEI) is not considered sensitive. However, app stores and the tools they use focus on detecting the unauthorized collection of device-specific data, providing almost no coverage for user-specific data. This issue is primarily caused by the limited capabilities of their tools to identify user-specific data. App stores' tools can easily detect device-specific data by monitoring a fixed set of system-level APIs that emit the data. But their tools are not capable of identifying user-specific data due to the contextual nature of the data to each app. For example, P9 mentioned:

"In fact, for us [a business-to-business (B2B) app], user data such as national ID, passports, phone numbers, and family info are considered sensitive data... But Android ID, Mac addresses, IMEI are not."

Popular apps are reviewed more strictly than unpopular apps. Interviewees reported that different apps can undergo different levels of privacy review by app stores. For most unpopular apps, app stores usually run automated analyses to detect their privacy violations. However, they apply additional manual analysis to popular apps, such as DiDi (a leading taxi-hailing app) and Meituan (the most used food-delivery app in China), which are used by nearly everyone in the country. One reason behind the different reviews is that the government-level privacy review (SPRC privacy review) tend to focus on popular apps with a large user base in China. Hence, app stores follow this pattern and perform extra manual analysis on popular apps. For instance, P5 said:

"For less well-known apps, the review process is primarily automated... There can be exceptions for particularly famous applications with a wide user base, such as Didi, Meituan, or Douyin. These popular apps often undergo some extra manual review."

Automated analysis is more efficient, but often fails to reveal privacy violations hidden in deeper program paths (e.g., requiring more user interactions to trigger), whereas manual analysis can complement the detection of these violations by exploring deep paths. Thus, unpopular apps are not evaluated as thoroughly as those popular apps, leaving questions about the extent of privacy assurance for these unpopular apps, which also collect personal information from end users.

The functionalities offered by third-party SDKs do not align with the privacy review requirements. Third-party SDKs play a crucial role in the supply chain of almost every app. When integrating these SDKs, interviewees anticipated incorporating only the functionalities required by their apps to meet the privacy compliance requirement in the privacy reviews. However, interviewees reported that SDKs often introduce unnecessary functionalities. For instance, P11 described a situation where their app initially needed an SDK solely for displaying maps based on user location data. Nevertheless, P11 ended up integrating a multi-functional SDK that not only displayed maps but also included voice recording features. The issue arises because the SDK must be used all-or-nothing, preventing P11 from selectively enabling only the necessary features. As a result, this led to the collection of unnecessary personal data, which is deemed

redundant and a violation in the privacy review. This challenge reflects the limitation of third-party SDKs and the challenges posed to privacy compliance, as they lack the flexibility to be configured and customized to the specific needs of apps:

"For example, your app requires location access functionality, while other apps may need recording or other features. Considering the variety of apps, they only offer one SDK, but it's used in different scenarios in different apps... For third-party SDKs, it's not feasible for them to customize an SDK specifically for your app's needs."

4.2.2 Yesterday's Compliance, Today's Noncompliance

Frequent updates to app review specifications make previously compliant apps noncompliant. The frequent changes of app review specifications of app stores have posed extra challenges to app developers. Five interviewees (P1, P3, P5, P14, P18) reported experiences with frequent changes in their apps' compliance status. In other words, an app initially identified by app stores as privacy-compliant can swiftly become non-compliant due to the updates in the app review specifications. Consequently, the app must undergo an unexpected rectification process, potentially requiring re-submission to app stores. This incurs a significant cost in terms of resources, money, and time to the app's provider, like what P5 said:

"There was a time when Bluetooth information was not considered personal data, but within a month, it was reclassified as such, which put us in a difficult situation, because we have to adapt accordingly"

Complicating the problem is the use of open-source tools. App developers often want to check their apps using open-source tools before submitting to privacy reviews. However, these tools are not always updated to catch up with the changes in the privacy review specifications. As a result, an app that these tools reported as compliant can have violations in the privacy reviews. For example, P11 said:

"Many issues arise from the tools not being updated promptly, then submissions were returned after review."

Constant updates to the apps make long-time privacy compliance unattainable. App providers need to regularly update their apps to keep up with technological advances and enhance the user experience. However, these updates can potentially introduce privacy violations to the apps. Interviewees noted that many app updates are delivered through dynamic features that don't require the apps to be resubmitted to app stores. This creates challenges for privacy enforcement from the perspectives of both app stores and app providers.

Currently, app stores only review the snapshot taken during the initial app submission and lack practical ways to monitor and review dynamic updates for privacy concerns. As a result, an app that was compliant at the time of submission may no longer be compliant due to subsequent updates. App stores, identified by SPRCs as partially responsible for the apps they distribute, cannot provide a reliable guarantee to app users about the privacy status of apps, even those they have reviewed. For instance, P18 mentioned that:

"Because those updates are not approved by them [app stores], nor will there be reviews... they will not know that the app has been updated"

Second, these app updates also pose challenges for app providers striving for privacy compliance. Three interviewees (P6, P9, P12) pointed out that their apps have such updates, and thus it is infeasible to maintain privacy compliance all the time. In particular, P12 explained that, as part of a security testing team, conducting privacy reviews for these app updates was infeasible due to the sheer volume of items to test. Due to this, P12 believes that achieving complete privacy compliance is not possible:

"However, we can't guarantee 100% compliance since there are too many items to test. An app might be compliant at the time of testing, but later additions of new features or modules could result in non-compliance. Therefore, compliance is time-bounded, or it can only be approximated by removing major issues, but there is no absolute and long-term privacy compliance."

4.2.3 Lack of Institutional Support from App Providers

Lack of support for studying privacy laws. Achieving privacy compliance requires a deep understanding of privacy laws, provisions, and periodical SPRC-related administrative notices issued by the government agencies. Whenever the government agencies issue an administrative notice for SPRCs, the review specifications will be updated, and the app developers are required to update their understandings as well. Ideally, these legal and governmental documents should be translated by legal professionals first before consumed by app developers. Nevertheless, four interviewees (P8, P9, and P10 in app developer roles, and P15 in a security engineer role) reported that they had to invest a significant amount of effort studying and tracking changes in the laws by themselves. These interviewees work at companies of different sizes: P8's company has 5,000+ employees, while P9's and P15's companies have 20+ and 100+ employees, respectively. This indicates that both large and small companies lack support for studying privacy laws. For instance, P10 complained about the complexity of legal terms, and highlighted that there should have been some legal professionals to help them decipher specific terms applicable to them and piecing them together into actionable items for engineers. However, the app providers attempted to minimize costs by not hiring a legal professional and asked app developers to take on the responsibility of studying and interpreting the laws. Additionally, participants reported that statements are lengthy and designed to cover a broad range of mobile apps. As the app developer for a specific app, they must read all the statements, figure out the specific statements applicable to their app, and translate the statements into concrete technical requirements based on

his own understanding. Lacking professional legal and privacy support not only increases burdens for app developers but can also lead to erroneous or biased understanding since most engineers do not have expertise in laws. For instance, P10 said that:

"the documents are often lengthy and complex... [There is a need] to distill some useful points for developers like us. Simplify them, then list them one by one, so we can check against these points. Translate them into actionable items that developers can easily implement. Identify which legal clauses and regulations we need to adhere to... it requires piecing several parts of laws together."

Lack of resources to self-validate privacy compliance. Participants complained that they had to develop tools on their own to self-validate privacy compliance before the government and app store privacy reviews. As the cost of failing the privacy review is huge, such as being publicly notified and unlisted from the app stores, app providers hope to self-detect potential privacy violations in their apps before officially submitting for app stores' or government's review. The self-detection requires a testing environment and a set of privacy violation detection tools, similar to PrivacySentry [6], and Google Checks [27]. App developers were expected by their institutions to develop these tools on their own if they want to self-detect their apps. However, app developers mostly specialize in implementing core app functionalities. They may not know how to build a testing environment, or deploy tools to assess an app's compliance with privacy regulations. They lack dedicated institutional resources, such as tools and privacy testers, to help them validate their apps' compliance status. As a result, app developers, after implementing the main functionalities, are further tasked with proving that the functionalities are privacy-compliant. They are either compelled to rely on open-source privacy violation detection tools or to learn the skill set and implement their own tools. The former option provides no guarantee, as open-source tools are from third-party and unknown entities, while the latter incurs significant learning curves and implementation efforts. Hence, having institutional resources (e.g., tools and dedicated testers) in place would significantly reduce the burden on app developers, and further simplify and enhance privacy compliance. For example, P9 mentioned that:

"For developers, ... the focus is typically on their own field, with only superficial knowledge about other domains, like basic understanding at best. For instance, tasks like packet sniffing are generally within the skill set of most programmers. However, developing a tool for detecting (privacy compliance) issues is not quite feasible, as this pertains to specialized tasks in the field of security."

Lack of support for effective communication. As the privacy reviews involve multiple stakeholders, such as app stores, third-party certifiers, government agencies, and app providers, interviewees (P3, P7, P11, P17, P18) highlighted the need to perform additional communication duties with these stakeholders about privacy review results, which happened to both small (e.g., P7) and relatively large companies (e.g., P3, P11, P17 and P18). The interviewees noted that these duties create a heavy burden beyond their regular job responsibilities, resulting in difficulties to address privacy violations within the allowed timeframe (i.e., 5 business days).

When an app is flagged for privacy violations, the developers first initiate internal discussions, by reaching out to legal and security teams to clarify the reports and determine whether they agree that a violation has indeed occurred. In the case of disagreement, the developers are then expected to convey the perspectives of the internal teams to app stores, third-party privacy certifiers or government agencies. After that, developers may need to persuade the reviewers that the reported violations are false positive. The aforementioned communication process is followed by additional communication required by technically reproducing the identified violations. For example, P11 mentioned that:

"First confirm the message [privacy violation reports] with legal teams... then send to security teams to confirm the reports... then confirm with legal team whether this [the feature that causes violation] is necessary... if we can not reproduce, we ask vendors [app stores] to reproduce. "

When privacy violations are caused by third-party SDKs (e.g., for P7), developers need to communicate the reported violations with the SDK developers and request a patched SDK. Unfortunately, this often turns out to be a challenging task that requires many rounds of communication, as many SDK providers are not responsive or not reluctant to patch their SDKs based on individual developer's requests.

In addition, interviewees reported that communicating as contractors about privacy compliance is most challenging. Some app developers worked as a contractor that develops apps for another company. When the app fails the privacy review due to noncompliance, the contractor developer is expected to explain the privacy violations to the company. However, the company is more concerned with the main functionalities of the app, and less interested in privacy compliance. There are often situations where functionalities conflict with privacy compliance (e.g., resulting in noncompliant data collection). To resolve the issue, developers need to engage in intensive communication to help the company understand the importance of complying with privacy regulations. For example, P17 told us:

"The biggest challenge lies in the requirement confirmation phase because sometimes clients focus more on functionality and may not care about privacy compliance, even though these must be addressed. So communication on requirements can incur significant costs."

Lack of fairness in accountability. App engineers are unfairly considered to hold the major responsibility or at fault for privacy violations. Upon the identification of privacy violations in an app, the app can be removed from app stores or notified by government. This could lead to a significant cost for the app providers, affecting their revenue and reputations. Interviewees

noted that when this happens, app engineers are often expected to be responsible for the privacy violations, without a fair discussion on factors such as business model and app design, that result in the privacy violations. They mentioned that app providers impose penalties on the app engineers who develop or test of the codes that triggers the violations, such as reducing their salary, bonus, and job safety. Moreover, government agencies only provide a short timeframe for app providers to rectify their apps. To achieve compliance and release their apps, app providers pressure app engineers to resolve these issues quickly, threatening them with salary penalties, which ends up with developers working overtime. For instance, P17 shared:

"The non-compliance issues in the app, which were not identified until reviews [by app stores], is actually quite serious within the company and will definitely result in lower performance evaluations."

During SPRCs, app engineers encounter various challenges, such as inconsistencies in privacy review reports and testing criteria, constant updates to review specifications, and a lack of institutional support from app providers.

4.3 RQ3: Solutions to Address the Challenges

To deal with the challenges in Section 4.2, interviewees developed a variety of strategies.

Performing pre-submission privacy certification. App providers face both financial and reputational costs due to privacy violations in their apps, such as apps being removed from app stores or being publicly notified upon the identification of privacy violations. Rather than being passively reviewed by external agencies, it is better for app providers to proactively discover privacy violations themselves.

App providers, exemplified by companies such as P1, P3, P6, P8, and P18, have adopted a pre-submission privacy certification process to reduce the chance of potential privacy violations, Most of these companies are relatively large, for example, P1, P3, P8, and P18 all have 1,000+ employees. This certification process, distinct from app developers' self-testing, often involves certifying the apps using professional and commercial certification tools from third parties, or conducting analyses within a dedicated security/privacy team. The app provider will send their pre-release apps to a dedicated security team that monitors all privacy-invading system interfaces and reports their findings for developers to address. P1 referred to this process as a "privacy fallback" or "last-minute privacy self-review" that catches as many issues as possible before the apps are publicized and become out of their control. For example, P1 noted that:

"The product [app] was designed and assessed by the legal team. However, the codes might not always align with the design. Therefore, after compiling the final product, a security team is needed for a comprehensive test. "

Offering privacy compliance training sessions. App engineers need more support from privacy and law professionals to better interpret the laws and eliminate confusion (Section 4.2.3). Seven interviewees – P5, P12, P13, P14, and P17 from relatively large companies with 1,000+ employees, and P6 and P7 from small companies – mentioned that their companies provided support through privacy compliance training sessions, led by either external or internal privacy law professionals.

P13 and P14 mentioned that their respective companies would invite officials from government agencies, including affiliated research institutions, to conduct training sessions for their employees. Given that the rationale behind privacy laws and guidelines is best understood by the officials who draft them, the training provided by the officials offers the most authoritative information for privacy compliance. This is confirmed by P13, who stated that these training sessions are effective since the officials would dissect the privacy compliance requirements, elaborate on the reasons for having them, and clarify who is responsible for meeting them, etc. Specifically, P13 mentioned that:

"they [the officials] actually break down and analyze every aspect for you. They present all the details, essentially laying out the standards and how they operate."

Six interviewees (P5, P6, P7, P10, P14, and P17) mentioned that their respective companies provide internal privacy compliance training for all employees. According to the interviewees, the training takes various forms and spans the entire duration of employees' service. Some companies incorporate past cases of privacy violations into the training, and integrate the training into the onboarding process of new employees, to ensure that they are privacy-prepared before commencing their actual duties. Additionally, these companies organize regular privacy trainings for product and engineering teams in order to help employees stay informed about new privacy updates. These internal training sessions are customized to meet the specific business needs of each company. Therefore, interviewees often feel that they get better awareness of privacy compliance after the training, like what P14 said:

"We also provide training during the onboarding of new employees... we conduct regular security training sessions related to compliance... We ensure timely synchronization if there are new standard requirements."

Collective sense-making on privacy compliance. Since all the apps in the app stores have to be reviewed for privacy compliance, developers for different apps have to go through the same privacy review process, fostering collective sense-making and knowledge sharing among privacy engineers. Additionally, achieving privacy compliance involves the interplay of multiple domains such as engineering, privacy, and legal. It has become a challenging task for which no individual possesses all the knowledge required for resolution. Consequently, a community with different stakeholders in privacy compliance has been formed, including app developers, law experts, devel-

opers working for third-party certifiers and developers working for app stores. Such communities enable app developers to collaborate with each other and with other types of stakeholders in making sense of privacy violations. This process is supported by online social media groups (e.g., on WeChat) and forums.

Five interviewees (P1, P8, P11, P12 and P13) have actively participated in collective sense-making through various means. Interestingly, all five of these interviewees work for relatively large companies with 1,000+ employees, which potentially suggest that employees from these companies are more active in sharing knowledge. Firstly, after addressing a privacy violation, they often publicly share information about their privacy violation and the techniques used to address it. This aids others facing similar privacy issues in quickly identifying potential solutions.

Secondly, when confronted with a newly reported violation lacking a straightforward solution, they would post the violation on social media groups or forums. Members on these platforms then engage in discussions, offering potential solutions in response to the post. In most cases, these discussions lead to effective resolutions swiftly. In addition to asking questions, they also participate in discussions about the violations of other companies.

Thirdly, they share updates on privacy review specifications and discuss the technical implications of these updates. These communities have become an essential, if not the only, source for small-sized companies to receive practical guidance for privacy compliance. For example, P12 told us:

> *"I think this group is very useful. Whenever anyone has questions, I've noticed that everyone is quite enthusiastic. You can just raise your question, and everyone can offer solutions based on your situation. If you were to ask other companies [instead of asking in the groups], there might be delays depending on their availability, the companies may hold back information, or they ask for a fee."*

Building privacy compliance into SDLC. Interviewees highlighted that building privacy compliance into the software development life cycle (SDLC) helps avoid privacy violations. This will avoid app developers being soly responsible for privacy noncompliance results. Rather than relying primarily on app developers' implementation, six interviewees (P1, P7, P11, P12, P13, and P18) reported that their companies involve two or more departments in different phases of SDLC in order to achieve privacy compliance. We did not observe any notable differences caused by company size, since the interviewees are from both small and relatively large companies. They emphasized the importance of testing privacy during the software testing phase, and noted that they consider privacy in the app's feature design phase, which allowed their company to avoid privacy violations at the early stage of software development, rather than having to reactively respond to reported violations. For example, P18 said:

> *"[Privacy compliance] is considered in all steps. We focus on ensuring that any changes in documentation are coordinated with development. ... Testing, whether using previously employed methods or new ones, is conducted to ensure consistency with policies and regulations."*

To address the challenges in SPRCs, app engineers perform pre-submission privacy certification, participate in privacy compliance training sessions, foster collective sense-making and knowledge sharing, and integrate privacy compliance into the SDLC.

4.4 RQ4: Positive Changes and Concerns

Here we summarize several positive impacts that interviewees are generally agreed upon, and the remaining public concerns with the privacy law enforcement campaigns.

4.4.1 Positive Changes

Reduction of privacy-invading apps. Despite the challenges discussed in Section 4.2, six interviewees (P1, P2, P3, P7, P11, and P12) personally felt that the enforcement of privacy laws has reduced the number of privacy-invading apps and restricted the abuse of sensitive user data. P11 mentioned that, prior to SPRCs, app providers, regardless of the types of their apps, attempted to collect as much user data as possible to build complete user profiles, and such data collection is now "not as common as before". P3 shared his before-SPRCs experience participating in the development of a flashlight app that aggressively accessed users' calendars and subscribed them to unauthorized charges. He highlighted that today's users can feel more assured due to the enforcement of privacy laws. Furthermore, from the perspective of an average user, P12 detailed three concrete positive changes resulting from the enforcement of privacy laws: 1) app privacy policies are becoming clearer and more comprehensive, 2) app user interfaces provide improved control over privacy (e.g., through runtime data collection requests and toggles for personalized ads), and 3) banking apps utilize secure keyboards to safeguard user input. Specifically, P12 mentioned that:

> *"First and foremost, you can see that privacy policies have been clearly laid out, which includes complaint channels, feedback methods, processing times, and collected information, allowing users to understand the policies at a glance... Secondly, from a user experience perspective, the requests for permissions and the ability to toggle features such as personalized ads... Then, for financial apps, the secure keyboards are much safer to use than the standard system keyboards, right?...Thus, with the introduction of national laws, there's no doubt that things will continue to improve."*

The participants' positive feelings about the reduction of privacy-invading apps resonate with recent app privacy reports from independent agencies [24,31] and academic research [36], which, for example, note a decrease in apps collecting device

identifiers such as IMEI and MAC, and an increase in apps obtaining user consent for data processing since the launch of SPRCs.

Growing agreement on the significance of privacy among app engineers. By informing app engineers about privacy-violating apps and compelling them to address these issues, the enforcement of privacy laws exposes app developers to essential privacy principles. This helped to cultivate a consensus on the importance of safeguarding user privacy. Not too long ago, stakeholders in mobile apps perceived the collection of user data as commonplace, exemplified by the statement made by the CEO of Baidu in 2018, suggesting that Chinese users were willing to trade privacy for convenience, safety, and efficiency [54]. Seven interviewees (P1, P3, P5, P11, P12, P14, and P16), however, emphasized their commitment to the "minimum necessary rule", a fundamental enforcement requirement, to ensure that they minimize data collection in alignment with their specific business needs whenever it occurs. P7 observed a change in the mindset of app developers regarding the enforcement of privacy laws. Initially, some developers resisted addressing privacy compliance issues because of the additional engineering work involved. However, they later acknowledged the significance of privacy compliance, citing "*what industry leaders should do*", which resulted in quicker responses to such issues:

> *"Resistance to privacy compliance and rectification actions did exist, but the situation has improved now... They [app developers] resisted because too much work to do... Most developers focus on their own staff, but privacy compliance is industry leader's considerations and is critical... Nowadays, developers are capable of understanding privacy compliance. They can quickly provide feedback on the issues, which are then promptly addressed, and they are even willing to engage in communication."*

Ongoing adaptation of privacy enforcement increases in-depth compliance. Privacy law enforcement is continually being strengthened to promote comprehensive privacy compliance, with the incorporation of more stringent rules that extend into previously uncovered user cases. According to P4 and P18, new enforcement rules are introduced to achieve both privacy and usability simultaneously. Apps are now mandated to request explicit consent for using privacy-sensitive permissions. These requests must include an option to cancel, provide clear explanations for the necessity of the permission through non-deceptive messages, and be presented in a manner that does not disrupt the user experience. P16 highlighted that privacy compliance is expanding its scope to cover business flows between apps and third parties. In cases where apps redirect users to external web pages and user data is collected on these pages, new rules require apps to inform users of the data collection before users can navigate to such web pages:

> *"If one of our services incorporates a function from a third-party contractor, and that contractor's interface requires users' personal information without a clear notification popup, it would be considered a violation... it is mandatory to clearly inform them about such actions."*

Moreover, third-party SDKs were initially viewed as black boxes, posing challenges for app developers in addressing privacy violations within them. The evolution of privacy enforcement has streamlined the handling of these SDKs. In particular, government agencies began directly detecting privacy violations within the SDKs and reporting them to the SDK providers. As indicated by the interviewees (P4, P7), this change was effective: many third-party SDKs are now proactively pursuing compliance similar to apps, and developers feel less concerned about using these SDKs.

4.4.2 Remaining Concerns

Potential techniques to circumvent SPRCs. The major concerns, as expressed by six interviewees (P4, P9, P10, P12, P15, P17), are the potential for privacy-invading apps to circumvent privacy enforcement through various means. P9 and P15 noted that, owing to the open nature of the Android platform, privacy-invading apps can be distributed with any ways (such as a downloadable link posted online) other than app stores that require privacy compliance. These apps can still impact a significant number of victim users, e.g., through referrals of popular social media platforms. P17 referred to the scandal of the Pinduoduo app, the most used C2B e-commercial app in China, that collects user data by exploiting operating system vulnerabilities [53], and speculated that similar bypass techniques might be employed by other companies without being detected. P10 reported that it is a common practice for large companies to support cloud-side configuration in their apps. During app reviews, they disable privacy-invading behaviors using this configuration, and only re-enable them after receiving approval from app stores (similar to [37]). Specifically, P10 mentioned that:

> *"This approach [bypassing detection] is widespread. For example, most companies employ a strategy where they place settings in the cloud... They deactivate these settings when the apps are under review, and then once the app passes the store's review, they reactivate them."*

Manipulation of privacy policies may lead to false compliance. When an app collects unnecessary sensitive user data, privacy regulations prohibit it to ensure compliance. However, P4, P12, and P15 highlighted instances where app providers continued collecting data. They added seemingly reasonable but deceptive statements to the app's privacy policies to justify the need for such data collection. In most cases, the app can still be published on app stores since the stores essentially permit any privacy practices listed in the privacy policies, as long as users agree. This manipulation of privacy policies is due to either innocent app developers who copy the privacy policies of other compliant apps, hoping it helps them become compliant as well, or malicious parties unethically

manipulating privacy policies. For instance, P4 said:

"Platforms [app stores] will not detect this [excessive data collection described in the privacy policy]. Because from the platform's perspective, they assume that the user has read that privacy policy. Yes, that's the standard procedure. As long as they [app stores] know there won't be any legal risks for the platforms, they generally allow it."

Interviewees report that SPRCs bring several positive changes, such as the reduction of privacy-invading apps, growing agreement on the significance of privacy among app engineers, and increased compliance due to the ongoing adaptation of privacy enforcement. However, app engineers are also concerned about the presence and use of techniques to evade privacy enforcement.

5 Discussion

Suggestions for SPRC-based privacy enforcement. SPRCs are large-scale campaigns under the directives of central authorities that involve various stakeholders, such as app providers and app stores, in the privacy enforcement process. As illustrated in Section 4.4.1, several app engineers reported positive changes based on their experience and perceptions, such as in reducing the explosion of privacy-invading apps and building agreement on the significance of privacy among app engineers. However, these positive changes do not come cheap. In this study, interviewees frequently reported that enforcement pressure has unfortunately been largely shifted onto app developers. These developers often find themselves ill-prepared for the diverse range of tasks they are now required to handle, such as studying privacy laws, communicating, and conducting compliance self-testing. The root cause of these difficulties lies in the absence of a robust mechanism (or process) within app providers to effectively coordinate (human) resources according to their expertise in privacy compliance. For example, offloading the task of studying laws to legal teams and the responsibility of communication to program managers, thus relieving app developers of these efforts. In the long term, it would be beneficial for app providers to establish a formal and sustainable process that guides multiple departments to collaborate seamlessly in order to ensure privacy compliance.

Furthermore, government agencies have successfully motivated app providers to address privacy violations through reporting and imposing heavy penalties, such as app removal from stores. However, resolving these violations requires a thorough understanding of privacy laws. While government agencies are the primary source of information for app providers, this study suggests they should have gone extra mile educating especially smaller companies. While larger firms may host training sessions with government officials, smaller companies, like P9's, often lack resources for such initiatives. Therefore, increasing accessibility to these sessions would greatly benefit smaller companies. Also, while SPRCs benefit from scalability and rapid sanctioning, they lack the procedural safeguards of privacy laws in other countries (e.g., those involving court procedures). Adding mechanisms to enhance assurance for companies facing incorrect or unfair judgments during sanctioning could be beneficial.

Implications to the enforcement of other privacy laws. SPRC-based enforcement represents an effort to enforce Chinese privacy laws with increased investment in administrative and public resources. Applying SPRCs directly to the privacy laws of other countries can be challenging due to factors such as differences in governmental structure and available resources. However, since the privacy laws of China and other countries share strong similarities [55], we believe that adopting at least some of the best practices from SPRC-based enforcement may help address certain persistent concerns in enforcing other laws. An example of this practice is highlighting the responsibility of app stores to conduct app privacy reviews. In some countries, app stores are not expected to ensure privacy compliance of apps through proactive privacy testing, but rather rely on self-compliance, for instance, apps self-claim their data practices via the Google Play's Data Safety section [28]. Given that self-regulation has almost stagnated [8], requiring app stores to launch systematic privacy reviews on their apps can be helpful.

Limitation discussion. This study focuses on app engineers and does not include other stakeholders involved in app privacy compliance, such as app stores, third-party privacy certifiers, and government agencies (as discussed in Section 4.1.1). Therefore, our findings reflect only the perceptions of app engineers and may not fully capture the broader landscape. For instance, insights into how app stores review popular versus unpopular apps, as well as their outsourcing of privacy reviews (as noted in Section 4.2), are based on app engineers' personal perceptions and limited exposure to these processes. They may not have complete knowledge of app store review procedures or whether such popularity-based review criteria actually exist. Consequently, the accuracy of these insights should be further validated by involving app store representatives. Nevertheless, our findings remain valuable. By focusing on the perspectives of app engineers, who are key stakeholders in app privacy compliance, including designing, testing, and implementing privacy controls, we establish an initial understanding of the problem space, and explore app engineers' understanding of SPRCs, the challenges they face, and their assessment of these concerns. Even if some bias exists, the fact remains that app engineers are impacted by SPRCs and face significant challenges in their roles, indicating the need for additional support to facilitate their work. As a next step, we plan to conduct a multi-stakeholder exploration (e.g., through focus groups and co-design sessions) to generate a more comprehensive and balanced understanding of SPRCs.

Additionally, the app engineers we interviewed may have self-censored their responses due to company policies, government oversight, or concerns about potential negative impacts

on their careers, which could introduce bias into our findings. While we discussed various challenges and complaints reported by app engineers in Section 4.2 (e.g., inconsistencies in privacy review reports, frequent changes to app review specifications, and lack of institutional support), our findings may lack a more comprehensive and candid discussion of criticisms regarding SPRCs. For example, these challenges and complaints are primarily directed toward app stores, third-party privacy certifiers, and their own companies, with no direct criticism of the central government, despite the fact that SPRCs are government-initiated. This lack of criticism toward the central government may be due to self-censorship, with app engineers potentially avoiding any negative commentary about the government out of concern for the potential impact on their careers. As a result, the self-reported data from these engineers may be incomplete and fail to fully reflect their true opinions about the government-led SPRCs. During our interviews, we took several steps to mitigate this bias, such as anonymizing responses, ensuring confidentiality, building rapport and trust with interviewees, and asking behavior- or situation-based questions to encourage more open responses. Despite these efforts, the findings may still provide only a partial view of app engineers' perceptions of SPRCs. Nevertheless, our study offers an initial glimpse into app engineers' views on SPRCs. We recommend that future research incorporate non-self-report methods, such as discourse analysis of public forums like Stack Overflow, to complement the interview findings and provide a more comprehensive perspective.

Our study is limited in scalability. Given the exploratory nature of the study, we adopted interviews with a small sample (18 participants) to probe open-ended and in-depth nuances, details and reasons behind app engineer's' opinions and practices in app privacy compliance. While this small sample is common in interview studies and reached thematic saturation, a larger sample is inevitably helpful to improve the scalability and representativeness of the findings. We acknowledge this limitation and hope to expand the scalability through methods like surveys in future.

6 Related Work

Research on the enforcement of privacy laws. With privacy law enforcement comes the question of its outcomes. Previous research uses retrospective and comparative methods to address this. For example, one line of research, represented by GDPRxiv [64], Saemann et al. [57], and Wolff et al. [78], collects information on past privacy law violations, and then conducts aggregated analyses or case studies to gain a better understanding of these violations (e.g., what privacy principles were commonly violated). Another line of research compares the apps, websites, or their privacy policies posted before and after the enactment of privacy laws [8,23,36,40,71], in order to measure the impacts of the enforcement of privacy laws. These studies yield a series of observations. For example, many more apps started to implement consent for data collection [36] and reduce the amount of data sharing [23]. Some studies show that privacy policies provide better transparency by covering more data practices with improved visual representations [40], while others have slightly contending observations, i.e., privacy policies have doubled in size and become more difficult to read [8]. Unlike the above studies that conduct retrospective or comparative analysis on the violation reports and apps, this study investigates the workflow, challenges, solutions, and overall results of the Chinese privacy law enforcement through the lens of app-related engineers, thanks to the deep involvement of them in the privacy compliance.

Research on techniques to aid privacy compliance. Both preventive and detective approaches have been developed in academia and industry to help achieve privacy compliance. Examples of preventive approaches include visual and structured representations and modeling of privacy laws to guide organizations in privacy management [69,70], automated tools to perform GDPR-compliant operations on legacy systems [4], an information flow tracking framework that supports privacy enforcement policies [32], and tools for automatically generating compliant privacy policies based on the analysis of app behaviors [80,85], etc. On the other hand, detective approaches are mostly driven by reported noncompliant privacy practices. For example, many prior studies proposed techniques to identify violations caused by privacy policies through flow-to-policy analysis [9, 13, 58, 83]. Other techniques aim to address specific types of noncompliance, such as checking the absence of explicit and freely given consent before data collection [34, 35, 48, 49]. In addition to that, commercial tools, such as Google Checks [27], Data Theorem Mobile Secure [68], AppCensus [1], and NowSecure Platform [2], have been recently introduced with capabilities to check the accuracy of privacy labels that developers self-report on app stores. Notably, none of the techniques or tools proposed so far claim to support full compliance detection for any privacy laws. The participants in this study may not directly use these techniques or tools, but they reported using open-source or commercial tools designed with similar methodologies.

Research on the challenges to privacy compliance. Previous research studies have extensively explored the challenges of achieving genuine privacy compliance in the process of EU/US privacy law enforcement, with most of them conducted through surveys or interviews with privacy stakeholders [5,7,10,11,29, 33,38,61,62,65,72,74]. Major challenges identified in these studies include: 1) the disconnection between technical implementations and general privacy principles [5, 33, 62, 65, 74], 2) failures in the interactions between engineers and legal experts [11, 29], and 3) a lack of knowledge about third-party SDKs being used [7, 38], and etc. The enforcement of Chinese privacy laws is based on SPRCs, involving a more extensive range of stakeholders and more frequent/complex interactions between them (which do not appear in the enforcement of US/EU privacy laws). This allows us to report a set of unique challenges that manifest in SPRC-based enforcement 4.2.

7 Conclusion

Recent years have seen significant positive changes due to the enactment of privacy laws. However, regulators are often under-resourced and have limited bandwidth to investigate the large number of apps. In contrast, since 2019, China has implemented Special Privacy Rectification Campaigns (SPRCs) to address widespread privacy issues in its mobile app ecosystem. The campaigns feature large-scale privacy reviews of apps and impose strict sanctions for identified violations. Despite some reports on SPRCs, the effectiveness and potential issues of these campaigns remain largely unclear. This paper seeks to evaluate this new campaign-style privacy enforcement approach and offer insights for future law enforcement practices. Through 18 semi-structured interviews with app-related engineers involved in SPRCs, we report new understanding about their process, challenges, solutions, and the impact of these large-scale campaigns. Our findings reveal the operational workflow of SPRCs and the challenges faced by app developers in compliance with these campaigns. Despite developers' adoption of technical and behavioral solutions to overcome these challenges, concerns persist regarding the effectiveness of SPRCs in addressing all privacy violations.

8 Acknowledgments

We would like to extend our heartfelt gratitude to the shepherd and the anonymous reviewers for their invaluable insights and constructive comments on our work. This work is funded by the National Key Research and Development Program (No.2022YFB4501300), National Natural Science Foundation of China under Grants 62202194. This work was supported by Ant Group through CCF-Ant Research Fund.

References

[1] AppCensus. https://appcensus.io.

[2] NowSecure Platform. https://www.nowsecure.com/products/nowsecure-platform/.

[3] Complete guide to gdpr compliance. https://gdpr.eu, 2023.

[4] Archita Agarwal, Marilyn George, Aaron Jeyaraj, and Malte Schwarzkopf. Retrofitting gdpr compliance onto legacy databases. *Proceedings of the VLDB Endowment*, 15(4), 2021.

[5] Abdulrahman Alhazmi and Nalin Asanka Gamagedara Arachchilage. I'm all ears! listening to software developers on putting gdpr principles into software development practice. *Personal and Ubiquitous Computing*, 25(5):879–892, 2021.

[6] Allenymt. privacy sentry. https://github.com/allenymt/PrivacySentry.

[7] Noura Alomar and Serge Egelman. Developers say the darnedest things: Privacy compliance processes followed by developers of child-directed apps. *Proceedings on Privacy Enhancing Technologies*, 4(2022):24, 2022.

[8] Ryan Amos, Gunes Acar, Eli Lucherini, Mihir Kshirsagar, Arvind Narayanan, and Jonathan Mayer. Privacy policies over time: Curation and analysis of a million-document dataset. In *Proceedings of the Web Conference 2021*, pages 2165–2176, 2021.

[9] Benjamin Andow, Samin Yaseer Mahmud, Justin Whitaker, William Enck, Bradley Reaves, Kapil Singh, and Serge Egelman. Actions speak louder than words:{Entity-Sensitive} privacy policy and data flow analysis with {PoliCheck}. In *29th USENIX Security Symposium (USENIX Security 20)*, pages 985–1002, 2020.

[10] Oshrat Ayalon, Eran Toch, Irit Hadar, and Michael Birnhack. How developers make design decisions about users' privacy: the place of professional communities and organizational climate. In *Companion of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing*, pages 135–138, 2017.

[11] Kathrin Bednar, Sarah Spiekermann, and Marc Langheinrich. Engineering privacy by design: Are engineers ready to live up to the challenge? *The Information Society*, 35(3):122–142, 2019.

[12] Virginia Braun and Victoria Clarke. Using thematic analysis in psychology. *Qualitative research in psychology*, 3(2):77–101, 2006.

[13] Duc Bui, Yuan Yao, Kang G Shin, Jong-Min Choi, and Junbum Shin. Consistency analysis of data-usage purposes in mobile apps. In *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*, pages 2824–2843, 2021.

[14] CAC. Cybersecurity law. http://www.cac.gov.cn/2016-11/07/c_1119867116.htm?subscene=0.

[15] CAC. Provisions on protecting the personal information of telecommunications and internet users. http://www.cac.gov.cn/2012-07/29/c_133142088.htm.

[16] CAC. Provisions on the scope of necessary personal information for common types of mobile applications. http://www.cac.gov.cn/2021-03/22/c_1617990997054277.htm.

[17] Sam Ruiqing Cao and Tobias Kretschmer. Regulation as opportunity: Proactive gdpr compliance in the us credit intermediation industry. *Available at SSRN 4778824*, 2024.

[18] Federal Trade Commission. Children's online privacy protection act. https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa.

[19] Federal Trade Commission. Federal trade commission. https://www.ftc.gov/.

[20] U.S. Equal Employment Opportunity Commission. Federal trade commission (ftc). https://www.eeoc.gov/federal-sector/reports/federal-trade-commission-ftc, 2024.

[21] California Consumer. alifornia attorney general's office. https://oag.ca.gov/.

[22] California Consumer. California consumer privacy act. https://oag.ca.gov/privacy/ccpa.

[23] Martin Degeling, Christine Utz, Christopher Lentzsch, Henry Hosseini, Florian Schaub, and Thorsten Holz. We value your privacy... now take some cookies: Measuring the gdpr's impact on web privacy. In *NDSS*, 2021.

[24] Deloitte. White paper on personal information protection for mobile applications (apps). https://www2.deloitte.com/content/dam/Deloitte/cn/Documents/risk/deloitte-cn-ra-mobile-app-personal-information-protection-white-paper-211028.pdf, 2021.

[25] Serge Egelman. Informing future privacy enforcement by examining 20+ years of coppa. *Harvard Journal of Law & Technology*, 37(3), 2023.

[26] Leo A. Goodman. Snowball sampling. *The Annals of Mathematical Statistics*, 32(1):148–170, 1961.

[27] Google. Checks. https://checks.area120.google.com.

[28] Google. Provide information for google play's data safety section. https://support.google.com/googleplay/android-developer/answer/10787469?hl=en#data_types.

[29] Stefan Albert Horstmann, Samuel Domiks, Marco Gutfleisch, Mindy Tran, Yasemin Acar, Veelasha Moonsamy, and Alena Naiakshina. "those things are written by lawyers, and programmers are reading that." mapping the communication gap between software developers and privacy experts. *Proceedings on Privacy Enhancing Technologies*, 1:151–170, 2024.

[30] iJiami. ijiami. https://www.ijiami.cn/.

[31] jiayouanke. 2022 annual report on personal information collection by apps. https://www.secrss.com/articles/50964, 2023.

[32] David Klein, Benny Rolle, Thomas Barber, Manuel Karl, and Martin Johns. General data protection runtime: Enforcing transparent gdpr compliance for existing applications. In *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security*, pages 3343–3357, 2023.

[33] Oleksandra Klymenko, Oleksandr Kosenkov, Stephen Meisenbacher, Parisa Elahidoost, Daniel Mendez, and Florian Matthes. Understanding the implementation of technical measures in the process of data privacy compliance: A qualitative study. In *Proceedings of the 16th ACM/IEEE International Symposium on Empirical Software Engineering and Measurement*, pages 261–271, 2022.

[34] Simon Koch, Benjamin Altpeter, and Martin Johns. The {OK} is not enough: A large scale study of consent dialogs in smartphone applications. In *32nd USENIX Security Symposium (USENIX Security 23)*, pages 5467–5484, 2023.

[35] Konrad Kollnig, Pierre Dewitte, Max Van Kleek, Ge Wang, Daniel Omeiza, Helena Webb, and Nigel Shadbolt. A fait accompli? an empirical study into the absence of consent to {Third-Party} tracking in android apps. In *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*, pages 181–196, 2021.

[36] Konrad Kollnig, Lu Zhang, Jun Zhao, and Nigel Shadbolt. Before and after china's new data laws: Privacy in apps. In *7th Workshop on Technology and Consumer Protection (ConPro'23)*, 2023.

[37] Yeonjoon Lee, Xueqiang Wang, Kwangwuk Lee, Xiaojing Liao, XiaoFeng Wang, Tongxin Li, and Xianghang Mi. Understanding {iOS-based} crowdturfing through hidden {UI} analysis. In *28th USENIX Security Symposium (USENIX Security 19)*, pages 765–781, 2019.

[38] Tianshi Li, Kayla Reiman, Yuvraj Agarwal, Lorrie Faith Cranor, and Jason I Hong. Understanding challenges for developers to create accurate privacy nutrition labels. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, pages 1–24, 2022.

[39] Timothy Libert, Lucas Graves, and R Nielsen. Changes in third-party content on european news websites after gdpr. *Reuters Institute for the Study of Journalism Reports: Factsheet*, 2018.

[40] Thomas Linden, Rishabh Khandelwal, Hamza Harkous, and Kassem Fawaz. The privacy policy landscape after the gdpr. *Proceedings on Privacy Enhancing Technologies*, 2020(1), 2020.

[41] MIIT. Miit. https://wap.miit.gov.cn/.

[42] MIIT. Notice of the miit on further improving mobile internet application service capabilities. https://www.gov.cn/zhengce/zhengceku/2023-03/02/content_5744106.htm.

[43] MIIT. Notice of the miit on launching special rectification actions for market order in the internet industry. https://tjca.miit.gov.cn/zwgk/dxhhlwgl/art/2021/art_84b25f1608b849079ba534be974964a0.html.

[44] MIIT. Notice of the miit on launching special rectification actions to intensify app infringement of user rights. https://www.miit.gov.cn/jgsj/xgj/gzdt/art/2020/art_c5f69af7882247198657b2ac6777ad62.html.

[45] MIIT. Special privacy rectification campaign. https://www.miit.gov.cn/jgsj/xgj/gzdt/art/2019/art_ebe83afcca4c430590c1a66cbbac1b21.html.

[46] MIIT. Means for determination of violations of laws and regulations in apps' collection and use of personal information. https://www.cac.gov.cn/2019-12/27/c_1578986455686625.htm, 2019.

[47] MIIT. Notification on apps involving user rights violations (first batch). https://www.gov.cn/xinwen/2019-12/20/content_5462577.htm, 2019.

[48] Trung Tin Nguyen, Michael Backes, Ninja Marnau, and Ben Stock. Share first, ask later (or never?) studying violations of {GDPR's} explicit consent in android apps. In *30th USENIX Security Symposium (USENIX Security 21)*, pages 3667–3684, 2021.

[49] Trung Tin Nguyen, Michael Backes, and Ben Stock. Freely given consent? studying consent notice of third-party tracking and its violations of gdpr in android apps. In *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*, pages 2369–2383, 2022.

[50] noyb. Your right to lodge a complaint under article 77. https://noyb.eu/en/your-right-lodge-complaint-article-77, 2024.

[51] NPC. Regulations on telecommunications. https://flk.npc.gov.cn/detail2.html?ZmY4MDgwODE2ZjNjYmIzYzAxNmY0MTE3YTQ2ZDE2OWU.

[52] The National People's Congress of China. Personal information protection law. http://www.npc.gov.cn/npc/c2/c30834/202108/t20210820_313088.html.

[53] Krebs on Security. Google suspends chinese e-commerce app pinduoduo over malware. https://krebsonsecurity.com/2023/03/google-suspends-chinese-e-commerce-app-pinduoduo-over-malware/.

[54] People's Daily Online. Robin li's "privacy for convenience" is disturbing. http://opinion.people.com.cn/n1/2018/0328/c1003-29894674.html.

[55] Emmanuel Pernot-Leplay and Emmanuel Pernot-Leplay. China's approach on data privacy law: A third way between the u.s. and the eu? (2020). *Penn State Journal of Law International Affairs*, 8(1), 2020.

[56] Irwin Reyes, Primal Wijesekera, Joel Reardon, Amit Elazari Bar On, Abbas Razaghpanah, Narseo Vallina-Rodriguez, Serge Egelman, et al. "won't somebody think of the children?" examining coppa compliance at scale. In *The 18th Privacy Enhancing Technologies Symposium (PETS 2018)*, 2018.

[57] Marlene Saemann, Daniel Theis, Tobias Urban, and Martin Degeling. Investigating gdpr fines in the light of data flows. *Proceedings on Privacy Enhancing Technologies*, 4:314–331, 2022.

[58] Nikita Samarin, Shayna Kothari, Zaina Siyed, Oscar Bjorkman, Reena Yuan, Primal Wijesekera, Noura Alomar, Jordan Fischer, Chris Hoofnagle, and Serge Egelman. Lessons in vcr repair: Compliance of android app developers with the california consumer privacy act (ccpa). *arXiv preprint arXiv:2304.00944*, 2023.

[59] Bangcle Security. Bangcle security. https://www.bangcle.com/.

[60] Cyber security. Miit: Nearly 3,000 illegal apps have been notified and removed from the shelves. http://finance.people.com.cn/n1/2022/0614/c1004-32445977.html.

[61] Awanthika Senarath and Nalin AG Arachchilage. Why developers cannot embed privacy into software systems? an empirical investigation. In *Proceedings of the 22nd International Conference on Evaluation and Assessment in Software Engineering 2018*, pages 211–216, 2018.

[62] Sean Sirur, Jason RC Nurse, and Helena Webb. Are we there yet? understanding the challenges faced in complying with the general data protection regulation (gdpr). In *Proceedings of the 2nd International Workshop on Multimedia Privacy and Security*, pages 88–95, 2018.

[63] Statista. Number of available applications in the google play store. https://www.statista.com/statistics/266210/number-of-available-applications-in-the-google-play-store/, 2024.

[64] Chen Sun, Evan Jacobs, Daniel Lehmann, Andrew Crouse, and Supreeth Shastri. Gdprxiv: Establishing the state of the art in gdpr enforcement. *Proceedings on Privacy Enhancing Technologies*, 4:484–499, 2023.

[65] Mohammad Tahaei, Alisa Frik, and Kami Vaniea. Privacy champions in software teams: Understanding their motivations, strategies, and challenges. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, pages 1–15, 2021.

[66] tc260. Personal information protection task force on apps. https://www.tc260.org.cn/piss/files/js2.pdf.

[67] Tencent. Wechat - free messaging and calling app. https://www.wechat.com/.

[68] Data Theorem. Mobile Secure. https://www.datatheorem.com/products/mobile-secure/.

[69] Jake Tom, Eduard Sing, and Raimundas Matulevičius. Conceptual representation of the gdpr: model and application directions. In *Perspectives in Business Informatics Research: 17th International Conference, BIR 2018, Stockholm, Sweden, September 24-26, 2018, Proceedings 17*, pages 18–28. Springer, 2018.

[70] Damiano Torre, Ghanem Soltana, Mehrdad Sabetzadeh, Lionel C Briand, Yuri Auffinger, and Peter Goes. Using models to enable compliance checking against the gdpr: an experience report. In *2019 ACM/IEEE 22nd International Conference on Model Driven Engineering Languages and Systems (MODELS)*, pages 1–11. IEEE, 2019.

[71] Tobias Urban, Dennis Tatang, Martin Degeling, Thorsten Holz, and Norbert Pohlmann. Measuring the impact of the gdpr on data sharing in ad networks. In *Proceedings of the 15th ACM Asia Conference on Computer and Communications Security*, pages 222–235, 2020.

[72] Dirk van der Linden, Irit Hadar, Matthew Edwards, and Awais Rashid. Data, data, everywhere: quantifying software developers' privacy attitudes. In *Socio-Technical Aspects in Security and Trust: 9th International Workshop, STAST 2019, Luxembourg City, Luxembourg, September 26, 2019, Revised Selected Papers 9*, pages 47–65. Springer, 2021.

[73] Benjamin Van Rooij. The campaign enforcement style: Chinese practice in context and comparison. In *Comparative Law and Regulation*, pages 217–237. Edward Elgar Publishing, 2016.

[74] Thomas Şerban von Davier, Konrad Kollnig, Reuben Binns, Max Van Kleek, and Nigel Shadbolt. We are not there yet: The implications of insufficient knowledge management for organisational compliance. *arXiv preprint arXiv:2305.04061*, 2023.

[75] Chenxi Wang. Legal and political practices in china's central–local dynamics. *Fudan Journal of the Humanities and Social Sciences*, 14(4):523–547, 2021.

[76] Jingyi Wang and Peng Wang. Campaign-style law enforcement in china: Causes and consequences. *Journal of Criminology*, 2024.

[77] Peng Wang. Politics of crime control: How campaign-style law enforcement sustains authoritarian rule in china. *The British Journal of Criminology*, 60(2):422–443, 2020.

[78] Josephine Wolff and Nicole Atallah. Early gdpr penalties: Analysis of implementation and fines through may 2020. *Journal of Information Policy*, 11:63–103, 2021.

[79] Bo Yin and Yu Mou. Centralized law enforcement in contemporary china: The campaign to "sweep away black societies and eradicate evil forces". *The China Quarterly*, 254:366–380, 2023.

[80] Le Yu, Tao Zhang, Xiapu Luo, and Lei Xue. Autoppg: Towards automatic generation of privacy policy for android applications. In *Proceedings of the 5th Annual ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices*, pages 39–50, 2015.

[81] Razieh Nokhbeh Zaeem and K Suzanne Barber. The effect of the gdpr on privacy policies: Recent progress and future promise. *ACM Transactions on Management Information Systems (TMIS)*, 12(1):1–20, 2020.

[82] Chunxiao Zhang. Imbalance in the institutional design of the chinese data governance system. *Law, Ethics Technology*, 2024.

[83] Kaifa Zhao, Xian Zhan, Le Yu, Shiyao Zhou, Hao Zhou, Xiapu Luo, Haoyu Wang, and Yepang Liu. Demystifying privacy policy of third-party libraries in mobile apps. In *2023 IEEE/ACM 45th International Conference on Software Engineering (ICSE)*, pages 1583–1595. IEEE, 2023.

[84] Shufeng Zheng. The application of facial recognition in china and india: Potential risks and regulation suggestions. *Journal of US-China Public Administration*, 18(3):115–132, 2021.

[85] Sebastian Zimmeck, Rafael Goldstein, and David Baraka. Privacyflash pro: Automating privacy policy generation for mobile apps. In *NDSS*, volume 2, page 4, 2021.

A Participants' information

Table 1 lists the background information of the participants in our interview.

Table 1: Participants' Background

No.	Comp. Size	City	Years	App Type	Department	Role
1	6,000+	Beijing	3+	Entertainment	Development	Developer
2	2,000+	Wuhan	3+	Finance	Development	Team leader
3	200,000+	Hangzhou	5+	Safeguard	Law	Policy interpreter
4	40+	Shanghai	6+	Tool	Development	Developer
5	4,000+	Beijing	5+	Security	Security	Regulator
6	100+	Shanghai	1+	Car system	Development	Developer
7	50+	Hefei	1+	Finance	Security	Security tester
8	5,000+	Beijing	4+	Estate	Development	Developer
9	20+	Shenzhen	3+	Education	Development	Developer
10	†	Singapore	6+	E-commerce	Development	Developer
11	10,000+	Hangzhou	1+	Social, Office, Education	Security	Security tester
12	3,000+	Beijing	2+	Finance	Development	Security tester
13	1,000+	Wuhan	3+	Tool	Technology	software manager
14	1,000+	Suzhou	4+	E-commerce	Security	Security tester
15	100+	Hangzhou	3+	Game	Security	Security engineer
16	20,000+	Zhengzhou	4+	Finance	Security	Security engineer
17	2,000+	Changsha	1+	Communication	Test	Test engineer
18	1,000+	Hefei	5+	News	Development	Technical leader

† P10 preferred not to disclose the company size.