
Cross-Country Exposure

Analysis of the MY2022 Olympics App

By Jeffrey Knockel

JANUARY 18, 2022

RESEARCH REPORT #149

Copyright

© Citizen Lab



Licensed under the Creative Commons BY-SA 4.0 (Attribution-ShareAlike licence). Electronic version first published in 2022 by the Citizen Lab.

This work can be accessed through <https://citizenlab.ca/2022/01/cross-country-exposure-analysis-my2022-olympics-app/>.

Document Version: 1.0

The Creative Commons Attribution-ShareAlike 4.0 license under which this report is licensed lets you freely copy, distribute, remix, transform, and build on it, as long as you:

- give appropriate credit;
- indicate whether you made changes; and
- use and link to the same CC BY-SA 4.0 licence.

However, any rights in excerpts reproduced in this report remain with their respective authors; and any rights in brand and product names and associated logos remain with their respective owners. Uses of these that are protected by copyright or trademark rights require the rightsholder's prior written agreement.

Suggested Citation

Jeffrey Knockel. "Cross-country Exposure: Analysis of the MY2022 Olympics App," Citizen Lab Research Report No. 149, University of Toronto, January 2022.

Acknowledgements

Funding for this research was provided by foundations [listed on the Citizen Lab's website](#). We would like to thank Mari Zhou for graphics design as well as Masashi Crete-Nishihata and Miles Kenyon for comments. We would like to thank an anonymous researcher for assistance in conducting background research and content analysis of relevant laws and policies for this report. Research for this project was supervised by Ron Deibert.

About the Citizen Lab, Munk School of Global Affairs & Public Policy, University of Toronto

The Citizen Lab is an interdisciplinary laboratory based at the Munk School of Global Affairs & Public Policy, University of Toronto, focusing on research, development, and high-level strategic policy and legal engagement at the intersection of information and communication technologies, human rights, and global security.

We use a “mixed methods” approach to research that combines methods from political science, law, computer science, and area studies. Our research includes investigating digital espionage against civil society, documenting Internet filtering and other technologies and practices that impact freedom of expression online, analyzing privacy, security, and information controls of popular applications, and examining transparency and accountability mechanisms relevant to the relationship between corporations and state agencies regarding personal data and other surveillance activities.

Contents

Key Findings	1
Introduction	1
Background	3
Privacy policy at a glance	3
Vulnerabilities in data transmission	5
Failure to validate SSL certificates	5
Failure to encrypt sensitive data	7
Disclosure	7
Updates	7
Censorship analysis	7
Discussion	10
Why was a keyword blocklist included?	11
Were the discovered vulnerabilities intentionally placed?	11
Does the insecure data transmission we discovered violate any laws or policies?	12
Are our findings surprising?	13

Read a translation of the report in [Simplified Chinese](#) and [Traditional Chinese](#)

Key Findings

- MY2022, an app mandated for use by all attendees of the 2022 Olympic Games in Beijing, has a simple but devastating flaw where encryption protecting users' voice audio and file transfers can be trivially sidestepped. Health customs forms which transmit passport details, demographic information, and medical and travel history are also vulnerable. Server responses can also be spoofed, allowing an attacker to display fake instructions to users.
- MY2022 is fairly straightforward about the types of data it collects from users in its public-facing documents. However, as the app collects a range of highly sensitive medical information, it is unclear with whom or which organization(s) it shares this information.
- MY2022 includes features that allow users to report “politically sensitive” content. The app also includes a censorship keyword list, which, while presently inactive, targets a variety of political topics including domestic issues such as Xinjiang and Tibet as well as references to Chinese government agencies.
- While the vendor did not respond to our security disclosure, we find that the app's security deficits may not only violate Google's Unwanted Software Policy and Apple's App Store guidelines but also China's own laws and national standards pertaining to privacy protection, providing potential avenues for future redress.

Introduction

The 2022 Winter Olympic Games in Beijing have generated significant controversy. As early as February 2021, over 180 human rights groups had called for governments to [boycott the Olympics](#), arguing that holding the Games in Beijing will legitimize a regime currently engaging in genocide against Uyghur people in China. Some governments including Canada, the United Kingdom, and the United States have pledged to [diplomatically boycott](#) the Games, meaning that these countries will allow athletes to compete at the Games but will not send government delegates to attend the event.

The International Olympic Committee (IOC), the organization responsible for organizing the Games, has been criticized for failing to uphold human rights. In December 2021, the United States House of Representatives voted [unanimously to condemn](#) the IOC and

stated that the IOC had violated their own human rights commitments by cooperating with the Chinese government. Following professional tennis player Peng Shuai's 2021 sexual assault [accusation](#) against Chinese Communist Party leader Zhang Gaoli and her subsequent disappearance, Human Rights Watch stated that "the IOC has vaulted itself from silence about Beijing's abysmal human rights record to active collaboration with Chinese authorities in undermining freedom of speech and disregarding alleged sexual assault." According to IOC documents, Zhang Gaoli [headed the steering committee](#) charged with securing and organizing the 2022 Games.

Internet platforms operating in China are [legally required](#) to control content communicated over their platforms or face penalties. Vague definitions of prohibited content are often called "[pocket crimes](#)" referring to authorities being able to deem any action as an offense. Such crimes are utilized by the Chinese government to restrict political and religious expression over the Internet. Chat and other real-time communications platforms operating in China typically perform automated censorship using a block-list of keywords whose presence in a message will trigger its censorship. [Previous work has found little consistency](#) in what content different Chinese Internet platforms censor. However, Internet platforms are [known to receive](#) censorship directives from various government offices or officials.

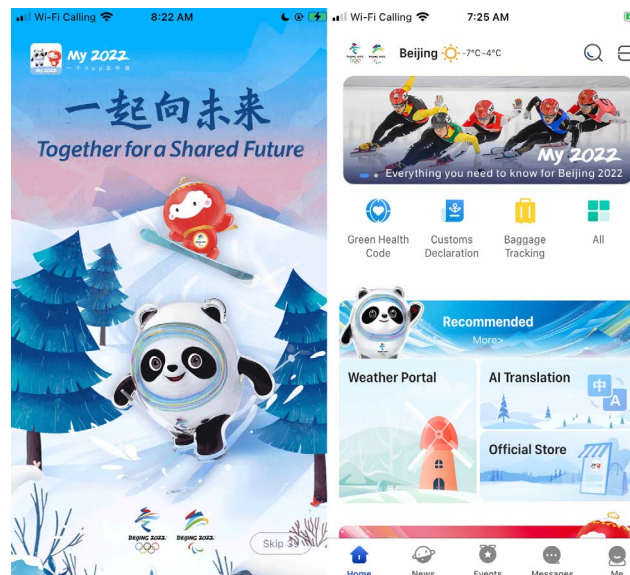


Figure 1: MY2022's splash screen and basic UI

In this report we analyze MY2022 (冬奥通), an app [required to be installed](#) by all attendees to the 2022 Olympic Games, including audience members, members of the press, and competing athletes. The app is multi-purpose, implementing a wide range of functionality including real-time chat, voice audio chat, file transfers, as well as news and weather updates about the Olympic Games. The app can also be used to submit required health

customs information for those visiting China from abroad, which includes submitting passport details, demographic information, as well as travel and medical histories.

Background

The 2022 Winter Olympic Games are expected to be held from February 4 to 20 in Beijing and towns in the neighbouring Hebei province in China. Due to the COVID-19 pandemic, China has decided to implement a “[closed-loop](#)” management system and daily testing. Additionally, all international and domestic attendees of the Games are mandated to download MY2022 14 days prior to their departure for China and to start monitoring and submitting their health status to the app on a daily basis.

Technical solutions such as app-based contact tracing have been increasingly used by countries around the world as a response to help mitigate the spread of the COVID-19 virus. However, as documented and [argued](#) elsewhere, app-based contact tracing and relevant technical solutions to public health issues are often [subject](#) to data breaches and exploitations as well as the potential risks of being expanded to wider ranges of social and political surveillance. It is therefore important to understand and evaluate the security and potential vulnerabilities of apps that collect and store highly sensitive data such as one’s medical information.

According to the Chinese government’s official [guide](#) on the Games, MY2022 was built by the Beijing Organizing Committee for the 2022 Olympic. [Public records](#) and [app store information](#) show that the app is owned by a state-owned company called Beijing Financial Holdings Group. MY2022 has a wide range of functionalities including tourism recommendations, GPS navigation, and COVID-19-related [health monitoring](#). One of the functions MY2022 includes is to collect a list of medical information for health monitoring, which includes users’ daily self-report health status, COVID-19 vaccination status, and COVID-19 lab test results.

Privacy policy at a glance

Before a company can make their application available on the Google Play store or Apple’s App store, they must first develop and publish a privacy policy to accompany the given application. We reviewed MY2022’s public-facing [privacy policy](#) document to understand what it states in relation to data collection, data storage, and data transfer. Overall, we found that MY2022 is fairly straightforward about the types of information it collects and with which third-party entities it shares information.

Third-party entity	Information shared	When / why share?
Huawei Technologies Co., Ltd	Device identifiers, cellular service provider information	If users are using Huawei devices
Xiaomi Inc.	Device identifiers, cellular service provider information	If users are using Xiaomi devices
Guangdong OPPO Mobile Telecommunications Corp., Ltd	Device identifiers, cellular service provider information	If users are using OPPO devices
Vivo Communication Technology Co. Ltd.	Device identifiers, cellular service provider information	If users are using VIVO devices
Meizu Technology Co., Ltd.	Device identifiers, cellular service provider information	If users are using Meizu devices
Tencent Holdings Ltd.	Cellular service provider information, device identifiers, installed apps on the device	To help users share information to WeChat and QQ
Weibo Corporation	Cellular service provider information, device identifiers, installed apps on the device	To help users share information to Weibo
AutoNavi Software Co., Ltd	Location, device information such as WLAN status, real-time location, device unique identifier, device model	To help users get real-time location and access lifestyle services on MY2022
iFlytek	Audio information, device status, device storage access, location access	When users use translation service on MY2022

Table 1: Summary of information sharing as disclosed in MY2022's privacy policy

For domestic users, MY2022 collects personal information including name, national identification number, phone number, email address, profile picture, and employment information and shares it with the Beijing Organizing Committee for the 2022 Olympics (see Table 1). For international users, the app collects a different set of personal identifiable information including users' demographic information and passport information (i.e., issue and expiration dates) as well as the organization to which they belong.

The [official Olympics Games Playbook](#) introduces MY2022 as a smartphone application for, among other things, health monitoring. MY2022 outlines in its privacy policy that it collects and uses users' daily self-report health status, COVID-19 vaccination status, and COVID-19 lab test results for such purposes. While the official Olympics Games Playbook outlines that personal data such as biographical information and health-related data may be processed by a list of entities including the Beijing 2022 Organizing Committee, Chinese authorities (including the Chinese National Government, local authorities, and other authorities in charge of health and safety protocols), the International Olympic

Committee, the International Paralympic Committee and “others involved in the implementation of the [COVID-19] countermeasures,” MY2022’s privacy policy itself did not specify with whom or with which organization(s) it would share users’ medical and health-related information.

Similar to other China-based apps we studied before, MY2022 outlines several scenarios where it will disclose personal information without user consent, which include but are not limited to national security matters, public health incidents, and criminal investigations. MY2022’s privacy policy did not specify whether each disclosure would be conducted under a court order or which organizations would potentially receive information.

Vulnerabilities in data transmission

In this section, we set out the two security vulnerabilities we discovered in MY2022 related to the security of the transmission of user data. First, we describe a vulnerability in which MY2022 fails to validate SSL certificates, thus failing to validate to whom it is sending sensitive, encrypted data. Second, we describe data transmissions that MY2022 fails to protect with any encryption.

We examined version 2.0.0 of the iOS version of MY2022 and version 2.0.1 of the Android version of MY2022. Although we were only able to create an account on and thus fully examine the iOS version of MY2022, from our best understanding, the vulnerabilities described below appear to exist in both the iOS and Android versions of MY2022.

Failure to validate SSL certificates

When a client uses SSL to connect to a server, SSL uses encryption and digital signature technology to provide both privacy and integrity to data in transit, protecting transmissions from being read or modified in between the client and the server. However, securing data in transit is by itself insufficient for guaranteeing either data privacy or integrity if a client could be deceived into connecting to a different host than the one intended, such as a malicious host in between the client and the intended server. To verify the authenticity of a server, SSL provides a method of securely receiving and validating certificates. By validating certificates, a client can ensure that data is secured not just in transit but that it is being sent from and received by the intended server.

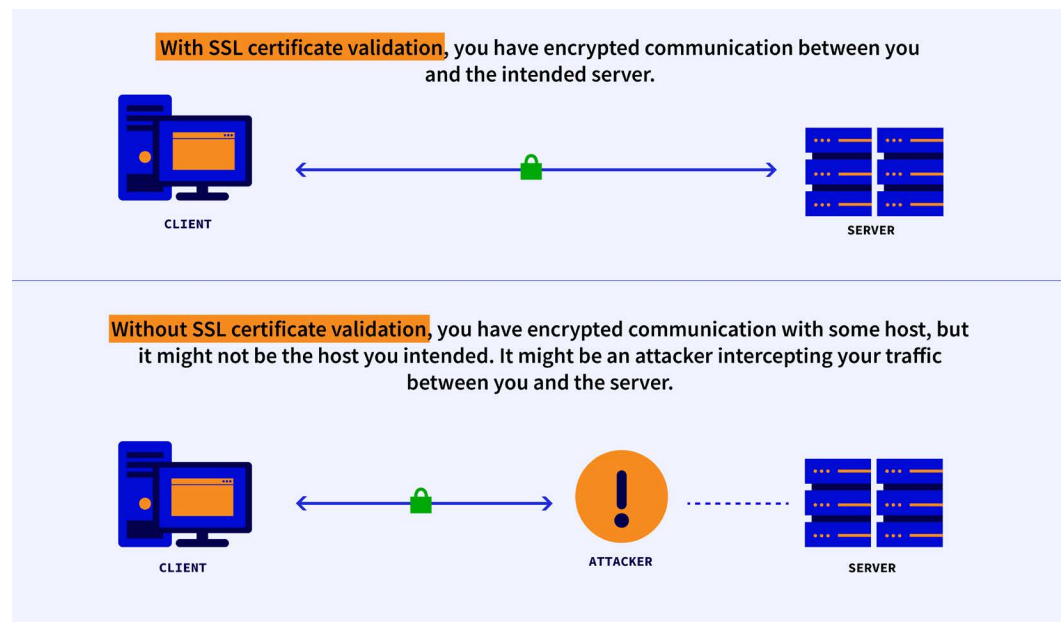


Figure 2: Infographic that explains the benefit of having SSL certificate validation.

Our analysis found that MY2022 fails to validate SSL certificates, allowing an attacker to spoof trusted servers by interfering with the communication between the app and these servers. This failure to validate means the app can be deceived into connecting to a malicious host while believing it is a trusted host, allowing information that the app transmits to servers to be intercepted and allowing the app to display spoofed content that appears to originate from trusted servers. Although we found that some connections were not vulnerable, we found that SSL connections to at least the following servers are vulnerable:

- my2022.beijing2022.cn
- tmail.beijing2022.cn
- dongaoserver.beijing2022.cn
- app.bcia.com.cn
- health.customsapp.com

For instance, since the app does not validate the SSL certificate for “health.customsapp.com”, an attacker, by interfering with the communication between MY2022 and “health.customsapp.com”, can spoof “health.customsapp.com”, enabling the attacker to read a victim’s sensitive demographic, passport, travel, and medical information sent in a customs health declaration or to send malicious instructions to a victim after completing a form. As another example, since the app does not validate the SSL certificate for “tmail.beijing2022.cn”, an attacker may use the same methods to read victims’ transmitted voice audio or file attachments.

Failure to encrypt sensitive data

In the previous section, we found that SSL was improperly implemented on many connections and thus vulnerable to attack. However, we also found that some sensitive data is transmitted without any SSL encryption or any security at all. We found that MY2022 transmits non-encrypted data to “tmail.beijing2022.cn” on port 8099. These transmissions contain sensitive metadata relating to messages, including the names of messages’ senders and receivers and their user account identifiers. Such data can be read by any passive eavesdropper, such as someone in range of an unsecured wifi access point, someone operating a wifi hotspot, or an Internet Service Provider or other telecommunications company.

Disclosure

On December 3, 2021, we disclosed the security issues we discovered to the Beijing Organising Committee for the 2022 Olympic and Paralympic Winter Games (66681024@beijing2022.cn), indicating that they have a deadline of 15 days to substantively respond to our disclosure and 45 days to fix the issues we identified before we would publicly disclose our findings. As of January 18, 2022, we have not received a response to our disclosure. We disclosed to the vendor according to our [vulnerability disclosure policy](#).

Updates

As of January 17, 2022, the developers released version 2.0.5 of the iOS version of MY2022 to Apple’s App Store. We analyzed it to see if the vulnerabilities we reported were fixed. However, we found that the issues we reported had not been resolved. Additionally, the app introduced a new feature called “[Green Health Code](#)” whose data transmissions were similarly vulnerable in that these transmissions were also instrumented using an SSL implementation that failed to validate SSL certificates. The “Green Health Code” feature asks for travel document information and medical history information similar to the information we had already found to be insecurely transmitted by the app’s vulnerable customs health declaration feature.

Censorship analysis

According to MY2022’s [description](#) in Apple’s App Store, the app implements a wide range of communication functionalities including real-time chat, news feeds, and file transfers. [In previous studies](#), we found the presence of censorship and surveillance keyword lists in different Chinese communication apps that provide similar services. Bundled with the

Android version of MY2022, we discovered a file named “illegalwords.txt” which contains a list of 2,442 keywords generally considered politically sensitive in China. However, despite its inclusion in the app, we were unable to find any functionality where these keywords were used to perform censorship. It is unclear whether this keyword list is entirely inactive, and, if so, whether the list is inactive intentionally. However, the app contains code functions designed to apply this list toward censorship, although at present these functions do not appear to be called. In the remainder of this section, we briefly analyze this list’s content.

Most of the 2,442 keywords are in simplified Chinese, with a small portion in Tibetan, Uyghur, traditional Chinese, and English. Similar to keyword lists we uncovered from other Chinese apps in [previous](#) studies, the majority of these keywords appear to be either politically motivated or social content referencing pornography (e.g., “成人论坛”, “adult forum”), swear words (e.g., “幹你娘”, “fuck your mother”), and illegal goods (e.g., “C4塑胶TNT”, “C4 plastic TNT”).

Chinese Keyword	Translation
犹太人是猪	Jews are pigs
中国人都是狗	Chinese are all dogs
捌玖陆肆纪念	Najiu Lusi Memorial
中共邪恶	CCP evil
viiv樂隊	viiv [June 4] band
习近平	Xi Jinping
中华人民共和国国务院	National Assembly of the PRC

Table 2: Selected Chinese keywords

The politically motivated keywords include negative references to the Chinese political system and intra-party power struggles (e.g., “胡江内斗”, “Hu (Jintao) Jiang (Zemin) infighting”), Falun Gong (e.g., “法轮大法好”, “Falun Dafa good”), and the Tiananmen Movement (e.g., “Tiananmen暴乱”, “Tiananmen riot”). Notably, the list also includes neutral references to the names of Chinese leaders as well as government agencies (e.g., “国家知识产权局”, The China National Intellectual Property Administration). See Table 2 for additional examples of Chinese language keywords and [here](#) for the full list.

Uyghur Keyword	Translation
ئابروي قۇرۇلۇشى	reputation building
ئۆكۈل سانجىش	injections
شەھەرنى توسۇش	block the city
قۇرئان-كەرىم	The Holy Quran
مەجبۇرى چارلاش	forced patrols

Uyghur Keyword	Translation
مەجبۇرى چىقىش	forced demolition
ياسالماقۇرلۇش	to be made

Table 3: Uyghur keywords

Tibetan Keyword	Translation
མགོན་པོ་	savior [one who can save us from suffering]
སྐབས་མགོན་	protector
གོང་ས་མཆོག་	His Holiness
དཔྲ་ལའི་བླ་མ་	Dalai Lama
ཏལ་ལའི་བླ་མ་	Dalai Lama
ཆེས་སྐར་	birthday
འབྲུངས་སྐར་	birthday [honorific]
སྐྱ་མཁའ་	the presence [of His Holiness]
སྐབས་བླ་མ་	protector teacher

Table 4: Tibetan keywords

Although live streaming app YY has censored keywords in Uyghur script and WeChat has censored keywords in both the [Uyghur](#) and [Tibetan](#) scripts, the inclusion of either Uyghur and Tibetan script keywords is uncommon in keyword lists, perhaps owing to the language barrier in curating keywords in these languages, and the keywords regarding Uyghur and Tibetan issues in most keyword lists are only in Chinese. While issues pertaining to the Chinese government's strict control over the Xinjiang region as well as the Uyghur ethnic groups have become a hot-button concern [surrounding](#) the Olympic Games, MY2022's Uyghur script keywords are not directly related to recent [controversies](#) such as the "[reeducation camps](#)". Rather, the Uyghur keywords generally relate to Uyghur issues or Islam commonly censored in China, such as the demolition of mosques in Xinjiang (see Table 3). MY2022's Tibetan script keywords generally relate to Tibetan Buddhism and the Dalai Lama (see Table 4). These topics are typically censored in China given the general sensitivity surrounding key political figures and activists, as well as China's sensitive relationship with the Dalai Lama and the existing [ethnic tensions](#) between minorities and the Han majority in China.

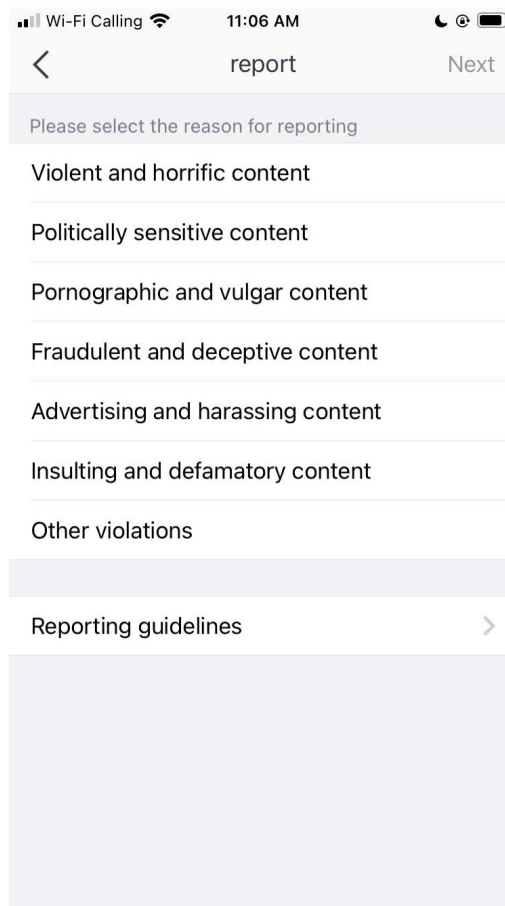


Figure 3: Screenshot of MY2022 showing reasons for reporting another user's message as inappropriate.

While the app's built-in censorship keyword list appeared unused, we did find that the app has reporting features that allow users to report other users' messages for political reasons (see Figure 2). The reporting feature is not novel or unusual for Chinese applications. However, it may potentially lead to non-transparent content removal and malicious reporting. [Previous work](#) on content moderation on WeChat's Public Account Platform suggests that companies often do not explain accurately why certain articles are deleted or whether an article was deleted due to the platform's user reports.

Discussion

In this section, we discuss our findings, including the purpose and motivations behind MY2022 including a keyword blacklist, whether the vulnerabilities we discovered in MY2022 were intentionally introduced, and whether MY2022 may be in violation of Chinese law or either Google's or Apple's policies.

Why was a keyword blocklist included?

It is unclear why MY2022 does not utilize its built-in blocklist to censor users' communications. On one hand, the inactiveness of the blocklist may be resulting from the same kind of accident that may have produced the app's failure to validate SSL certificates. On the other hand, the censorship may have been intentionally disabled, in a bid to hide the extent of China's censorship regime from outsiders or out of pressure from the IOC, who has [previously attempted negotiations](#) with the Chinese government over what content it can and cannot censor at the games.

Were the discovered vulnerabilities intentionally placed?

China has a history of [undermining encryption technology](#) to perform political censorship and surveillance and exploiting unencrypted network communications to [launch man-in-the-middle attacks](#). Furthermore, local Chinese governments routinely use [data interception technology](#) to sniff wifi traffic for surveillance purposes. As such, it is reasonable to ask whether the encryption in this app was intentionally sabotaged for surveillance purposes or whether the defect was born of developer negligence. However, the case for the Chinese government sabotaging MY2022's encryption is problematic.

For instance, the most sensitive information being handled by this app is submitted in health customs forms, but this information is already being directly submitted to the government, and thus there would be little instrumental rationality in the government intercepting their own data, as weaknesses in the encryption of the transmission of this information would only aid other parties. While it is possible that weakness in the encryption of health customs information was collateral damage from the intentional weakening of the encryption of other types of data that the Chinese government would have an interest in intercepting, our prior work suggests that insufficient protection of user data is [endemic to the Chinese app ecosystem](#). While some work has [ascribed intentionality](#) to poor software security discovered in Chinese apps, we believe that such a widespread lack of security is less likely to be the result of a vast government conspiracy but rather the result of a simpler explanation such as differing priorities for software developers in China.

A related hypothesis might explain how these flaws could be intentionally introduced while not the direct result of a government conspiracy but yet still an indirect result of government policies. While China's national firewall does not attempt to intercept SSL traffic, such interception technologies may be much more common at local levels for both political and non-political purposes, such as when using the networks of [cafes](#), [universities](#), or [one's employers](#). To use correctly-implemented SSL over such networks

intercepting SSL, a user must manually install an SSL certificate provided by the interception device. The MY2022 developers may have intentionally hamstrung their SSL implementation so that the app would continue to function over such networks, even if a user has not manually installed an interception SSL certificate. While we find this hypothesis plausible, we are unaware of any data to confirm it. However, we suspect that such interception technologies are more widely deployed in China versus other countries due to the [legal responsibility](#) that China delegates to companies and other entities to censor content on their networks.

The knee-jerk reactions against Chinese apps and suspicions of their censorship and surveillance capacities are to a large extent warranted as there exists extensive documentation of security flaws, privacy violations, and information controls on apps operated in China and internationally-facing apps developed by Chinese companies. It is worth noting, however, that the Chinese government has taken significant steps to rein in companies' invasive collections and poor handling of personal information, largely following global approaches to personal data protection.

Does the insecure data transmission we discovered violate any laws or policies?

Since the promulgation of the Cybersecurity Law in 2016, Chinese regulators have enacted [a series of](#) regulations, guidelines, and national standards including the [Personal Information Protection Law](#) (PIPL), [the Data Security Law](#) (DSL), the [Civil Code](#) to help build its [data governance regime](#). Despite the [policy priority](#) of national security over individual protection, these laws and regulations pertaining to data security and privacy nonetheless specify measures and remedies safeguarding violations by individuals, companies, and sometimes [state organs](#). MY2022, an app that is used primarily for COVID-19 contact tracing purposes, processes a wide range of sensitive personal information including users' passport information and health status. According to China's [national standard](#) on information security technology pertaining to health data, personal health and medical data should be transmitted and stored in an encrypted manner. Additionally, Article 51 of the PIPL stipulates that personal information processors shall adopt corresponding technical security measures such as encryption and de-identification to safeguard personal data. Article 27 of the DSL requires that processors of important data should specify the persons or organizations responsible for data security and protection. Hence, MY2022's insecure transmission of personal information may constitute a direct violation of China's privacy laws.

Apps on Android phones may be governed by two different sets of Google policies. If

an app is listed in Google's Play Store, the app is governed by [data safety policies](#) which include requiring developers to document which types of data are collected and whether they are encrypted. Even if an app is not listed in Google's Play Store, it is still covered by Google's broader [Unwanted Software Policy](#) which effectively applies to any phone with Google's Play Services installed. According to this policy, apps "must not collect sensitive information such as banking details without proper encryption". Our findings expose how MY2022 fails to properly encrypt sensitive information including passport details, demographic information, and travel and medical histories. Apps that violate the Unwanted Software Policy are liable to be blocked from installation by Google Play Protect.

As an app listed in Apple's App Store, MY2022 is also subject to Apple's [App Store Review Guidelines](#). These guidelines require that apps "should implement appropriate security measures to ensure proper handling of user information collected... and prevent its unauthorized use, disclosure, or access by third parties." Our findings expose how MY2022's security measures are wholly insufficient to prevent sensitive data from being disclosed to unauthorized third parties. Apps that violate Apple's App Store guidelines may be delisted from the store.

Are our findings surprising?

In light of our previous research, our findings analyzing MY2022, while concerning, are not particularly surprising for apps operating in China and sometimes apps developed by Chinese companies. For many years, China did not have laws or specific agencies that oversee private companies' collections and protection of personal data. Chinese apps ranging from banking apps to video streaming platforms have been [found](#) to excessively collect sensitive user data, often without user consent. [Previous studies](#) have also found that compared to their internationally-facing versions in jurisdictions with more comprehensive data protection frameworks, China-based mobile apps tend to have less ideal user protection and privacy policies. While we found glaring and easily discoverable security issues with the way that MY2022 performs encryption, we have also observed similar issues in Chinese-developed [Zoom](#), as well as the [most popular Chinese Web browsers](#). MY2022's functionality to report other users for "politically sensitive" expression is common in [other Chinese apps](#), and, while we found bundled a list of censorship keyword terms capable of stifling political expression, such lists are near ubiquitous in [Chinese chat apps](#), [live streaming apps](#), [mobile games](#), and even [open source software](#). In light of previous work analyzing popular Chinese apps, our findings concerning MY2022 are, while concerning, not surprising.

