PRIVACY AND POWER AROUND THE BEIJING 2022 OLYMPICS: LEGAL AND POLITICAL PERSPECTIVES

Qianye Zhang*

Abstract: The Beijing 2022 Olympic Winter Games launched a smartphone application, MY2022, to monitor the health status of participants in order to control the spread of the SARS-CoV-2 virus. However, Citizen Lab, a Canadian research institute, found that the protections of the data storage and transmission process of this application were either weak or completely unencrypted, leading to users' privacy being at risk of potential leaks. In addition, the study found that the app's instant messaging feature contained a list of sensitive words that had not been activated. Although Citizen Lab's report pointed out that these security vulnerabilities might be unintentional failures by developers rather than an intentional arrangement by the Chinese government, the criticisms were still widely cited by international media, bringing pressure on the Chinese Olympic Committee and the Chinese authorities. Despite the fact that both the International Olympic Committee and the Chinese Olympic Committee declared the bugs had been fixed since the release of the initial research report, Beijing has much to learn beyond the scope of technical issues.

Keywords: SARS-CoV-2, MY2022, privacy, cybersecurity, censorship

* Consultant, the World Bank.

Table of Contents

I. BACKGROUND

The 2022 Beijing Winter Olympics will begin on February 4, 2022. China, the authoritarian state that will be the first to hold both summer and winter Olympics, is under scrutiny by international human rights watchers and liberal states, given its record of large-scale domestic surveillance[1] and the vulnerability of the West[2] .

As the world approaches three years of the COVID-19 pandemic, countries have begun to respond to the pandemic very differently. While North America and some nations in Europe have started to reopen the economy and loosen control over social distancing, lockdown, and contact tracing, other countries , such as China, are still treating coronavirus with strictly-enforced measures.

China has been boasting its capacity in controlling the spread of the virus to a limited scale despite its large population size and high population density. China's successful efforts in combatting the pandemic can be at least partially attributed to the development of digital technology. The "health code"[3] and contact tracing technology allow local authorities to track users' travel history, test results, body temperature and other health data and private information such as their phone and ID number. When a positive case is diagnosed and detected, the authorities can quickly target close contacts of the positive case and install strict quarantine measures to limit further spread of the coronavirus.

When the Winter Olympics approached, China extended its domestic experience of fighting the pandemic to its handling of the Olympics, designing a smartphone-based application, named "MY 2022", for all Olympics-related personnel.

According to the introduction on Apple Store and Google Play Store, My 2022 "consists of two sectors, namely the Beijing 2022 Games services and the city guide services."[4] MY2022 asks users to submit several types of private information, including passport ID number, phone numbers, and health data such as self-reported health status, COVID-19 vaccination status, and test results.

The International Olympic Committee (IOC) says the download of the app is not compulsory, yet according to the Beijing Winter Olympic Games playbook, before traveling to Beijing, participants will be "required to download the 'My 2022' mobile

---

[1] Buckley, Wang and Bradsher, Living by the Code: In China, Covid-Era Controls May Outlast the Virus, The New York Times, Jan 30, 2022. Available at: https://www.nytimes.com/2022/01/30/world/asia/covid-restrictions-china-lockdown.html?_ga=2.80595031.1726735185.1643854743-442066510.1578563656

[2] Neary, Bryce (2022) "Tech and Authoritarianism: How the People's Republic of China is Using Data to Control Hong Kong and Why The U.S. is Vulnerable," Seattle Journal of Technology, Environmental & Innovation Law: Vol. 12 : Iss. 1 , Article 5. Available at: https://digitalcommons.law.seattleu.edu/sjteil/vol12/iss1/

[3] See the explanation given by the China Center for International Knowledge and Development (CIKD), available at: http://www.cikd.org/chinese/detail?leafId=212&docId=1339

[4] See the introduction of MY 2022 on Apple Store, available at: consists of two sectors, namely the Beijing 2022 Games services and the city guide services https://apps.apple.com/nz/app/my2022/id1548453616

application and use the Health Monitoring System (HMS) inside"[5] to monitor users' health prior to their departure.

The IOC stated that the 'MY 2022' "is an important tool in the toolbox of the COVID-19 countermeasures,"[6] aiming to mitigate the spread of the disease within the Olympic village and especially among athletes. It also contains other functions that provide information unrelated to COVID-19, such as game schedules, tourist and travel guidance, and can serve as an instant messaging tool.

II. CYBERSECURITY FLAWS OF MY2022

The Citizen Lab, a Canada-based technology research institute, revealed in a report the existence of several security vulnerabilities. According to the Citizen Lab, at least two security vulnerabilities were detected that could put users' privacy at risk of being leaked.

The lab claims that "MY2022 fails to validate SSL certificates, which are "digital infrastructure that uses encryption to secure apps and ensures no unauthorized people can access information as it is transmitted,"[7] which can be exploited by ill-intentioned third parties to trick users into visiting unintended servers and malicious sites.

It also discovered that MY2022 fails to encrypt sensitive data. These 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."[8]

Based on their previous research and analysis, the lab researchers concluded that the data security failures suffer from the generally-weakened Chinese app ecosystem, and are "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."[9] However, this conclusion is missing in most of the media coverage.

III. POTENTIAL CENSORSHIP

The lab report also claims it discovered a file titled "illegalwords.txt" containing a list of 2,442 sensitive words. The listed words can be divided into two groups: those that contain pornographic meaning, illegal goods, or swear words, and those deemed politically sensitive in China's political context.

The report said they were "unable to find any functionality" to activate the censorship on the keywords. The report made two assumptions explaining why the sensitive keywords are listed but remain inactive. One assumption is that it may result

---

5 See Column "Answer Playbook" in Row #187, Beijing 2022 Playbook, available at: https://olympics.com/athlete365/app/uploads/2021/12/2021.12.13-Beijing-2022-Playbook-Version-2-QAs.pdf

6 The IOC's response to DW's media inquiry. Available at: https://www.dw.com/en/ioc-reacts-to-cybersecurity-concern-over-beijing-my-2022-phone-app/a-60466680

7 Jeffrey Knockel, Cross-Country Exposure Analysis of the MY2022 Olympics App, The Citizen Lab. Available at: https://citizenlab.ca/2022/01/cross-country-exposure-analysis-my2022-olympics-app/

8 Id 7.

9 Id 8.

from "the same kind of accident that may have produced the app's failure to validate SSL certificates."[10] The other assumption is that the censorship may have been intentionally disabled out of political concerns or compromises with the IOC.

The report was released on Jan 18, 2022, approximately two weeks before the opening ceremony of the Winter Olympics. International media quickly followed up and covered the concerns. The lab said they notified the Olympic Committee on Dec 3, 2021, of a 45-day period to resolve the issues, but the updated versions of MY2022 still contained the issues as of Jan 16, 2022.

On Jan 20, the Beijing 2022 Organizing Committee announced that all the security flaws had been fixed, without further mentioning whether the sensitive keywords list were removed from the app code. The IOC also responded that the app had been approved by Google Play and Apple Store and had no critical vulnerabilities.

IV. LEGAL ISSUES RELATED TO SECURITY FLAWS AND CENSORSHIP

Analyzing the security vulnerabilities of MY2022 per the Citizen Lab is complicated due to the diverse nationalities of its users and the different rules and regulations of the various platforms where it is displayed online.

A. Probable Violation of China's National Laws?

Since the promulgation of the Cybersecurity Law of the People's Republic of China in 2016, the legislative progress of cybersecurity, personal privacy protection, data protection, etc., has advanced at a faster pace.

The most applicable laws identified by the Lab's report are the Personal Information Protection Law (PIPL) and the Data Security Law (DSL).

Article 51 of the PIPL requires that personal information processors shall adopt "corresponding technical security measures such as encryption and de-identifi- cation" to "ensure that their personal information processing activities are in compliance with laws and administrative regulations."[11]

Article 27 of the DSL requires that processors of important data should specify the persons or organizations responsible for data security and protection.[12]

If the Beijing 2022 Organizing Committee did not fix the security issues, and should the flaws lead to severe consequences, it may violate the relevant articles of the PIPL and the DSL.

The PIPL states clearly the scenarios under which it could be a violation and be faced with penalties. In the Legal Liability part, Article 66 of the PIPL requires that, in the event of a violation of the law, responsible entities "shall order the violator to make

[10] Id 9
[11] The Personal Information Protection Law of the People's Republic of China, 2021. http://en.npc.gov.cn.cdurl.cn/2021-12/29/c_694559.htm
[12] The Data Security Law of the People's Republic of China, 2021.

corrections, give a warning, confiscate the illegal gains, and order the suspension or termination of provision of services by the applications that illegally process personal information."[13] A fine shall be imposed where the violator refuses to make corrections.

Article 6 of the PIPL provides remedial measures in the event of a violation of the law. Violators who fulfill their obligations and fix the security flaws can be exempted from penalties.

B. Censorship: Contradictory Articles in the Constitution

Although the sensitive keywords list is not activated to perform censorship in the MY2022, it is worth discussing the possibility of whether censorship could violate the Chinese Constitution in this context.

There are conflicting articles in the Chinese Constitution. Article 35 grants citizens the "freedom of speech, the press, assembly, association, procession and demonstration."[14] One can argue that Chinese participants can exert the rights promised by Article 35 and that it would be unconstitutional to activate the censorship and filter the sensitive keywords.

However, Article 28 of the Constitution also grants the state the right to "suppress treasonable and other criminal activities that endanger State security."[15]

In addition, Article 12 of the Cybersecurity Law of the People's Republic of China rules that users "must not incite subversion of national sovereignty, overturn the socialist system, incite separatism, break national unity, advocate terrorism or extremism, advocate ethnic hatred and ethnic discrimination, disseminate violent, obscene, or sexual information, create or disseminate false information to disrupt the economic or social order."[16]

The examples of the sensitive keywords given in the Lab report cover words and terms that could likely be deemed by the Chinese authorities as inciting, subversive, or advocating ethnic hatred. Hence, the app developer and the Beijing 2022 Organizing Committee could argue that the sensitive keywords list is legitimate according to Article 12 of the Cybersecurity Law and Article 28 of the Constitution.

C. Violating Online Platforms' Policies

The report further points out that the security bugs may also violate Google Play policy and Apple's app store policy. Violations of the policies could lead to the removal of the app.

---

[13] Id 11.
[14] Constitution of the People's Republic of China, 2004.
[15] Id 14.
[16] Cybersecurity Law of the People's Republic of China, 2017.

- Google's Unwanted Software Policy recommends in its "Snooping" session that "software must not collect sensitive information such as banking details without proper encryption."[17]

- App Store Review Guidelines by Apple also require in its "Data Security" session that "apps should implement appropriate security measures to ensure proper handling of user information…and prevent its unauthorized use, disclosure, or access by third parties."[18]

If there are no severe consequences of privacy leakage, it is fairly unlikely that Google or Apple would remove the MY2022 from their platforms. Both online stores set the tolerance policy to allow the developers to update their apps and fix the bugs in a given period following the platform's notice. Google's Unwanted Software Policy mainly targets malware. MY2022 should not be categorized as "malware" due to the nature of its function, and neither platform had delisted the app prior to its submission of the updated version on Jan 29, 2022.

V. THE DILEMMA OF CONTACE TRACING

It has to be acknowledged that hosting the Olympics during the COVID-19 pandemic era is fundamentally different than it was for previous Winter Games. Broadly speaking, what Beijing faces today is not so much a technical problem as an ideological rivalry between individual freedom and state power. The rivalry poses a challenge to almost every country that has the capability to conduct contact tracing.

Since the beginning of the COVID-19 pandemic, contact tracing has been recommended by many professionals as one of the most effective methods to slow down the spread of the coronavirus, and it has been proven true in countries where obedience and compliance are social norms. However, contact tracing to speed up the detection of possible positive caseshas become a controversial measure in countries with liberal roots. Privacy issues aside, there are two major components of the public argument

A. Contact Tracing vs. Indicidualism

The goal of contact tracing is to uncover when a close contact might be a coronavirus-positive case, resulting in local authorities imposing quarantine measures or limiting the freedom to move. For liberal democratic countries, there is an ethical dilemma of conducting contact tracing. Health is considered a fundamental right of everyone.[19]To protect the right to health, state governments have to limit individual freedom, which in many cases led to lawsuits from citizens against their governments.[20]

---

[17] Google's Unwanted Software Policy, available at https://www.google.com/about/unwanted-software-policy.html

[18] Apple's App Store Review Guidelines, available at: https://developer.apple.com/app-store/review/guidelines/

[19] International Covenant on Economic, Social and Cultural Rights, Article 12(1).

[20] Some of the examples of noteworthy lawsuits can be found here: https://ballotpedia.org/Lawsuits_about_state_actions_and_policies_in_response_to_the_coronavirus_(COVID-19)_pandemic,_2020-2021

B. Contace Tracing vs. Effectiveness

For some countries that have tried to leverage digital contact tracing by developing contact tracing apps, it often leads to underperformance of the app and a waste of budgetary resources.

Tokyo is the other city so far that has held the Olympic Games since the beginning of the pandemic. Tokyo also faced challenges from the app used by Japanese residents to monitor users' health conditions. Japan regarded privacy protection as its top priority. International media did not interrogate the Japanese Olympic Committee over the security issue on the app, COCOA. Instead, many members of the Japanese media questioned the effectiveness of the app. Local media reported that the encryption made it "all but impossible for the government to grasp the actual number of notifications sent via the app,"[21] not to mention that there weren't enough downloads and self-reports to hit the 60% uptake ratio[22] that would make the contact-tracing app work in theory.

VI. THE LESSONS FOR BEIJING

The Citizen Lab report rightly states that the security vulnerabilities of MY2022 are likely the resultof the Chinese software ecosystem which generally doesn't prioritize privacy protection. The ensuing media coverage focused on the security issues of the app and the keywords list, without including that the report also mentioned that the security bugs might not be intentional outcomes of the design. Olympic Committees of participating countries such as the US, Canada, Germany and the Netherlands have encouraged their teams to use disposable phones while in Beijing, reinforcing the impression to the public that these Olympics are not trustworthy.

The deep-seated distrust towards the Chinese government and government-backed international events can be traced back to 2008 when Beijing held the summer Olympics. A US senator claimed that several international chain hotels had reported being wiretapped by Beijing without giving the specific brand of the hotels in hopes of protecting the hotels from retaliation[23].

From Beijing's perspective, the international image crisis of their 2022 Winter Olympics is not so much a technical issue as it is a political and ideological standoff between China and the liberal West. Beijing can dismiss all the charges against itself on surveillance, and still be confident with its own "Chinese path." Still, it has to regain some trust if it is keen on bidding for and hosting future international sporting events

---

[21] Tomohiro Osaki, Glitches and design flaws limit value of Japan's COVID-19 tracing app, The Japan Time, Feb 1, 2021. Available at: https://www.japantimes.co.jp/news/2021/02/01/national/science-health/cocoa-tracing-troubles/

[22] Research brief published on the Oxford University website. Available at: Digital contact tracing can slow or even stop coronavirus transmission and ease us out of lockdown (There needs to be a URL here for the website)

[23] Richard Cowan, China spying on Olympics hotel guests: U.S. senator, Reuters, Jul 30, 2008. Available at: https://www.reuters.com/article/us-olympics-china-spying/china-spying-on-olympics-hotel-guests-u-s-senator-idUSN2934051920080729

And technical correctness, rather than political correctness, should be the first step to regain global trust. The low-hanging fruit here is to promise better enforcement of privacy and data protection in a digital era.

Take the MY2022 as an example. According to Article 31 of the Government Procurement Law of the PRC, MY2022 is purchased from Beijing Financial Holding Group Co., Ltd., the authorized operator of the "Beijing Tong" app.

According to its introduction, the "Beijing Tong"[24] app has built a city-wide unified identity authentication system based on the concepts of identity access, data access, application access and people-to-people communications. The Beijing Tong app has 7 categories of practical functions, such as showing certificates, handling affairs, inquiries, payment, reservations, complaints, and communication.

Here lies reasonable speculation. MY2022 and Beijing Tong may be developed by the same team and MY2022 may have borrowed similar parts of codes from Beijing Tong. Data privacy might rank behind the priority on the developing team's agenda. Both the developing team and Beijing residents are used to neglecting privacy protection, which creates an ecosystem where sluggish privacy protection receives neither supervision nor punishment. With the Olympics, the situation can completely differ, as participants are used to different technology standards and privacy protocols.

The Beijing 2022 Organizing Committee also failed in proactively seeking to improve the function of the app. The Citizen Lab team said they had sent notice to the Organizing Committee in Dec 2021, and never received any response before the official release of the report, which created a public relations fiasco for Beijing.

The Lab report and the resulting media crisis provided a classic case study for China to learn how an honest mistake can lead to a major public image setback. It should be a warning sign to China's growing confidence.

China has become more confident and less patient in listening to the world, with its international status and economic power rising. As China gets deeply involved in the global agenda, "telling China stories well" is a reciprocal channel with the underlying requirements of listening to the world's needs as well. With privacy protection becoming an increasingly important issue globally, the state should improve their technology ecosystem's performance on data privacy-related policy and laws.

Although the IOC has insisted repeatedly that the Olympic Games are "politically neutral", the games are never short of politics. Athletes from across countries come not only to show their muscles, but to show the strengths of ideology as well. With China showing its interests and financial competitiveness in holding more sporting events, and becoming more stubborn and confident in its own path, the rest may have fewer choices other than "mitigating, or migrating"—either using a burner phone, or quitting the games held on this land.

[24] Introduction on the App Store. Available at: https://apps.apple.com/cn/app/%E5%8C%97%E4%BA%AC%E9%80%9A/id1158919706