PRIVACY AND POWER AROUND BEIJING 2022 OLYMPICS: LEGAL AND POLITICAL PERSPECTIVES¹

Zhang Qianye

Abstract

The Olympic Winter Games Beijing 2022 launched a smartphone application, MY2022, to monitor the health status of participants to control the spread of the virus. However, Citizen Lab, a Canadian research institute, found that the application has weak or unencrypted encryption in the data storage and transmission process, leading to users' privacy being exposed to potential leakage risk. 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 stated 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 for the Chinese Olympic Committee and the Chinese authorities. Despite that International Olympic Committee and the Chinese Olympic Committee declared to have fixed the bugs after the release of the research report, much beyond the technical failures awaits Beijing to learn.

I. Background

Beijing Winter Olympics 2022 is scheduled to 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 records of large-scale domestic surveillance² and the vulnerability of the West³ that are widely believed by international media. Third-year into the COVID-19 pandemic, countries react to the pandemic differently. While North America and some countries in Europe have started to re-

¹ Qianye, Zhang, Privacy And Power Around Beijing 2022 Olympics: Legal And Political Perspectives (Feb. 3, 2022) (unpublished manuscript, on file with The International Journal of Law Ethics and Technology).

² 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

³ 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/>

open the economy and loosen the control over social distancing, lockdown and contact tracing, other parts, such as China, are still treating coronavirus with strictly enforced measures.

China has been boosting its experience over limiting the interpersonal spread of the disease to a small scale relative to its large population size. The success over the combat against the pandemic can at least partially attribute to the development of digital technology. The “health code”⁴ and contact tracing technology allows local authorities to track users’ travel history, test results, body temperature and other health data and private information such as the 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 came near, China extended its domestic experience of fighting the pandemic to its handling of the Olympics, designing a smart-phone 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.”⁵ MY2022 asks users to submit several types of private information, such as passport ID number, phone numbers, and health data such as self-report 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 application and use the Health Monitoring System (HMS) inside”⁶ to monitor users’ health prior to their departure.

The IOC stated that the 'MY 2022' “is an important tool in the tool box of the COVID-19 countermeasures”⁷, aiming to mitigate the spread of the disease within the Olympic village and especially among athletes. It contains other functions that

⁴ 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>

⁵ 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

⁶ 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>

⁷ 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>

provide information such as game schedules, tourist and travel guidance, etc. It also can serve as an instant messaging tool.

II. Cybersecurity Flaws of MY2022

The Citizen Lab, a Canada-based technology research institute, has revealed in a report the existence of several security vulnerabilities. According to the Citizen Lab, at least two security vulnerabilities are detected that could put users' privacy to 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"⁸, which can be exploited by ill-intentioned third parties to trick users to visit 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."⁹

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"¹⁰. However, this conclusion is missed in most of the media coverage.

III. Potential Censorship

The lab report also claims it discovered a list of 2,442 sensitive words in a file under the name "illegalwords.txt". 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.

⁸ 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/>

⁹ Id 7.

¹⁰ Id 8.

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 from “the same kind of accident that may have produced the app’s failure to validate SSL certificates.”¹¹ 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 have notified the Olympic Committee on Dec 3, 2021, of a 45-day period, but the updated versions of MY2022 till Jan 16 still contained the issues.

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

IV. Legal issues related to the security flaws and censorship

Analyzing whether 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 platform where it is displayed online.

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 been advanced at a faster pace.

The most applicable laws identified by the Lab’s report are namely 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-*

¹¹ Id 9

cation” to “ensure that their personal information processing activities are in compliance with laws and administrative regulations”.¹²

Article 27 of the DSL requires that processors of important data should specify the persons or organizations responsible for data security and protection¹³.

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 under what scenarios could it 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 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*”¹⁴. A fine shall be imposed where the violator refuses to make corrections.

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

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 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*.”¹⁵ One can argue that Chinese Olympic participants can exert the rights promised by Article 35 and that it would be unconstitutional to activate the censorship and filter the sensitive keywords.

¹² 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

¹³ The Data Security Law of the People’s Republic of China, 2021.

¹⁴ Id 11.

¹⁵ Constitution of the People’s Republic of China, 2004.

However, Article 28 of the Constitution also grants the state the right to “*suppresses treasonable and other criminal activities that endanger State security*”¹⁶.

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*”¹⁷.

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

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.

- Google’s Unwanted Software Policy recommends in its “Snooping” session that “*software must not collect sensitive information such as banking details without proper encryption*”¹⁸.
- 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*”¹⁹.

¹⁶ Id 14.

¹⁷ Cybersecurity Law of the People's Republic of China, 2017.

¹⁸ Google’s *Unwanted Software Policy*, available at <https://www.google.com/about/unwanted-software-policy.html>

¹⁹ Apple’s App Store Review Guidelines, available at: <https://developer.apple.com/app-store/review/guidelines/>

If there are no severe consequences of privacy leakage, it is fairly unlikely for the online stores to remove MY2022. 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.

V. The Dilemma of Contact Tracing

It has to be acknowledged that the Olympics during the COVID-19 pandemic era is no longer the same as before. Broadly speaking, what Beijing faces today is not as much as a technical problem as it is 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 effective methods to slow down the spread of the coronavirus, and it has been proved to be true in countries where obedience and compliance are part of the social norm. However, contact tracing has become a controversial measure to speed up the detection of possible positive cases in countries with liberal roots. Privacy issues aside, there are another two major public disputes.

- Contact tracing vs. individualism

Contact tracing sometimes leads to a warning that certain close contact might be a coronavirus-positive case and then local authorities will impose quarantine measures or at least limit the freedom to move. For liberal democratic countries, there is an ethical dilemma of conducting contact tracing. Health is considered a fundamental right of everyone²⁰. To protect the right to health, state governments have to limit individual freedom, which in many cases lead to lawsuits from citizens against their governments²¹.

- Contact tracing vs. effectiveness

²⁰ International Covenant on Economic, Social and Cultural Rights, Article 12(1).

²¹ 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](https://ballotpedia.org/Lawsuits_about_state_actions_and_policies_in_response_to_the_coronavirus_(COVID-19)_pandemic,_2020-2021)

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 problem.

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 took privacy protection as its top priority. International media did not interrogate Japan Olympic Committee over the security issue on the app, COCOA. Instead, many 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"²², not to mention that there weren't enough downloads and self-reports to hit the 60% uptake ratio²³ that would make the contact-tracing app work in theory.

VI. The Lessons for Beijing

The Lab report rightly states that the security vulnerabilities of MY2022 are more of the outcome of the Chinese software ecosystem which generally doesn't prioritize privacy protection. Media coverage following this report focuses on the security issues of the app and the keywords list, without including what 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 recommended their team 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 the name of protecting the hotels from retaliation.

From Beijing's perspective, the international image crisis of this 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

²² Tomohiro Osaki, *Glitches and design flaws limit value of Japan's COVID-19 tracing app*, The Japan Times, Feb 1, 2021. Available at:

<https://www.japantimes.co.jp/news/2021/02/01/national/science-health/cocoa-tracing-troubles/>

²³ 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

itself on surveillance, and still be confident with its own “Chinese path”. Still, it has to regaining trust at least on occasions such as the international sports games it is keen on bidding and holding.

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, “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 Olympics, the situation can completely differ.

The Beijing 2022 Organizing Committee also failed in proactively seeking to improve the function of the app. The Citizen Lab 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 eventually led to a public relations fiasco for Beijing.

The Lab report and the media crisis is a latest 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 becomes more confident and less patient in listening to the world with its relative international status and economic power rising. As China gets deeply

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

involved in the global agenda, “telling China stories well” is a reciprocal channel with the underlying requirements of listening to the world’s need as well. With privacy protection becoming an increasingly important issue globally, the state should improve the 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 sports 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.