Dr. Chunyuan DING

China's Digital Health Code System to Fight COVID-19: A Trade-off between Public Health and Privacy

Today I'm going to talk about the China's digital health Code system. The reason for bringing me to this topic are twofold. First, COVID-19 epidemic requires and enables the government to make use of the information and the digital technologies for contact tracing in order to control the spread of the disease, which give rise to ethical and legal concerns on how to balance public health promotion and individual rights protection, in particular, right of privacy and autonomy. Second, as chairman has introduced, I'm working on tort law and health law for years, and one essential topic that can link these two fields of law is privacy issue in healthcare. China's digital health code system provides a good example for exploring this issue. So in this context of public health emergency, let's look at how to balance these competing interests.

So I'm going to talk about three issues. The first one is what is China's digital health code system running currently? The second one let's look at how Chinese law protects personal data and the third is about the tradeoff between the public health promotion and privacy protection.

In February, 2020, Chinese government encourage people to run to work, continue to work despite the COVID-19 outbreak, the Alipay health code was first introduced it to the city of Hangzhou by the local government, with the help of financial assistance company of Alibaba. Two days later, another internet giant in China, Tencent, also released its own version of health code in Shenzhen, where Tencent's headquarter is located. Within two months, the system has been rolled out nationwide, although different names of health code were given in various provinces and the cities. So how does the digital health code system work China? People are required to sign up a health code app through Alipay, or WeChat with real name, verification, fill in their health information and travel information, which is sent to

the central server. After central server receives all inflammation from terminal devices of user, the centralized system processes and analyzes all data, including those from healthcare, Telecom, transportation, online information sector, as well as the custom and immigration authorities. Then the central server, by utilizing big data and AI technologies, decided the health status of the users, who was assigned a color code, as you can see from this slide. Green, yellow, or red, that indicates their health status. So green code means the user is healthy, while the yellow and the red code indicate respectively middle and the high level of the infection risk, the users with yellow and the red code are forbidden to use public transportation or access to you public or commercial or work premises.

At the same time, the staff stationed in those premises will measure the temperature of everyone who enters the premise, check the color of individual health code, and sometimes require people to scan the location barcode in order to get to the real time geolocation information of the user. So if you look at the picture on the right, this is the entrance of an MTR station in city of Wuhan. So people are required to scan the location barcoding in order to report their geolocation information to the server.

The next question is what are the major functionalities of the Chinese system? It has actually two major functionalities. One is the contact tracing. And the second is quarantine. When the big data analysis determines certain users are COVID-19 diagnosed or suspected, or they're close contacted, their health code will then turn to yellow or red. Moreover, they had to stay at a home or assigned a hotel or hospital because without the green code - it's like the health passport, they can go nowhere.

So compared to the contact training apps used in other countries, such as Singapore, Australia, France, German, or the UK, Chinese one has full features. First, it collects massive data of different types, wide scope and a large amount of from almost the whole population.

Second, it adopts the roots of terminal device, central server, then to terminal device, and process the transmitted data in a centralized away. Third healthcare is QR code, which potentially holds a lot of personal data in an encoded form, or it can technically have linked to the database which contains personal data of users.

Finally, it generates a health code with different colors, as you have seen, rather than giving mere warning message to the users at risk, the yellow and the red code can deprive users of the right to physical autonomy.

So now let's move to the law legal part. In 2009, the crime of invasion of personal data privacy was edited by the seventh Amendment to criminal law. And then 2012, the standing committee of national people's Congress released their decision on strengthen online information protection, providing a very general principle to protect the online information of users.

Then one year later, the ministry of industry and information technology made the regulation on protecting the personal information of telecommunications and the internet users. And this law actually provided a set of rules on how to protect the personal data.

Then in 2016, the cyber security law is made by the standing committee of NPC which mainly address the issue of data security. And this year in May, the China's new civil code was made by the NPC, which contains a chapter titled “protection of privacy and a personnel data”. So we can see in the past decades, China has developed its own law on personal data protection. However, there is a big room for improvement, specifically we can look at the four aspects.

First, although the new civil code has a special chapter on protection of privacy and the personal data. It has only eight articles in total, far from a complete legal framework of data protection. Other rules scattered in different laws, regulations, rules, and the even judicial interpretations made by the SPC - Supreme People's Court. There is no special law in China, such as like the Hong Kong personal data protection ordinance, compared it to the OECD eight principles of data protection, the new civil code has not embraced the data quality principle, use limitation principle and accountability principle.

Second, the Chinese law, by and large, states the general principles, but lacks specific feasible rules for implementation, which has caused difficulties in effective implementation in practice.

Third, Chinese law does not establish a special public authority or organ in charge of data protection. The regulatory power is in fact divided in various public agency, depending on where a breach occurs.

So now we look at the third apart regarding the trade-off between public health promotion and the privacy protection. In a contest to have a COVID-19 pandemic, the governments of national level released a notice on effectively protecting personal information and using big data to support a joint prevention and control. And the second is made in May this year which is titled the information construction for communities' work on the prevention and control of new coronavirus and application guided jointly released by a number of public authorities of state council.

So in this two pieces of legislation and the government emphasized the voluntary basis, data minimization principle use limitation principle, as well as data security issue. However, neither of them addressed the balance between public health and privacy or data protection. If we compare the Chinese enactments of these two, and with the guidance on apps, supporting the fighting against the COVID-19 pandemic in relation to data protection, which was made by European commission in April this year, and this is the follow alike, we can see the constructions between these two solutions regarding making use of the technology to fight COVID-19.

So specifically the first point is relating to the collection of personal data. Although the two anatomists of Chinese governments emphasize the requirements of consent on a voluntary basis; in practice, it is mandatory for people to provide a personal data through a health code app, because without the green code, people cannot go anywhere or participate important events, such as attending high school entrance examinations. As a result, the whole population, regardless of their health conditions must give consent to data collection in order to avoid life inconvenience or other restrictions. The data subjects once providing their personal data to the centralized system, lose control over the sharing and the disclosure of their own data. On the countrary, EU's guidance required that app user must be in control of their personal data with respect to matters, including app installation, choices of functionalities, as well as decided whether or not to share proximity data.

Second, China's health code is system collects identity data, health, travel, and transportation data, geolocation data, and the like, although the government's enactments echo the data minimization principle, in effect, it adopts a strategy of rather being excessive than being inadequate. It is unclear whether the disclosure of data to the third-party user is subject to the same problem.

Then if you will look at the EU side, EU guidance emphasizes the data minimization and only allows the blue low energy communication data can be generated and processed, only if there is an actual risk of infection.

The third aspect is about the China's health code system failing to specify who is the data controller and who should it be responsible for the legal accountability. Because it contains massive data of different kinds, many public authorities are involved in the system. This is even so when the data are shared across local governments, when the personal information collected in the system is incorrect, diagnosed illegally or stolen or abused, the data subject has no idea about to whom, he or she should report the case, lodge complaints or seek remedies. Then if you will look at the EU's part, the guidance actually makes clear that national health authority as data controller also required involvement of data protection authority.

And the last one China's health code faces a threat to data security and accuracy, because all data are in centralized storage process and analysis. Moreover, unknown third parties are authorized to access to use the data; that's creating a high risk of unauthorized disclosure, hacking or abuse, the lacks of mechanism to ensure data quality control and to implemented data protection.

So if you look at the EU side, the EU guidance, actually, recorder proximity data can only store in user's device in an encrypted form. And also the key code must be regularly changed rather than actual device ID was sent to the system.

Okay. So finally we will look at what's the future of the health code system in China, this is the version of health code 2.0, which was advocated in the city of Hangzhou. The Alibaba's headquarter city. The new version collects more health information, including exercise, alcohol consumption, smoking, and sleeping. Most of the media reports in China and the general public in China give positive reaction towards it. The high tolerance of the Chinese society maybe explained from multiple perspectives in the context of China.

In interest of time, I shall stop here. Thank you!