September, 2020

Data, AI Governance, and COVID -19:

Medium and Long-Term Perspectives for Asia

CHINA

Yi Zeng
Chinese Academy of Sciences

Kang Sun
Chinese Academy of Sciences

Enmeng Lu
Chinese Academy of Sciences

SOUTH KOREA

Sangchul Park
Seoul National University

Yong Lim
Seoul National University

SINGAPORE

Mark Findlay
Singapore Management University

JAPAN

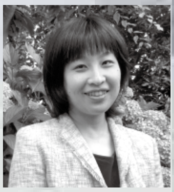

Arisa Ema
The University of Tokyo

Table of Contents

SINGPORE

Singapore and COVID-19 control – a tale of 2 cities?

JAPAN

Challenges of AI and Data Utilization and Governance in Japan Emerging from the COVID-19 response

Foreword

Arisa Ema

In response to the coronavirus (hereafter referred to as COVID-19) pandemic of 2019-20, various IT/AI technologies such as tracking app, contact confirming app, and facial recognition systems that automatically recognize images of appropriate social distances and urge caution are being promoted. However, these technologies raise concern about the balance between public benefits and individual privacy, and whether such measures will lead to new discrimination and prejudice. In Asian countries where the first wave of infection surged prior to other regions, various technical attempts have been implemented from an early stage, and measures are being taken with a view of medium and long-term prospects during the pandemic and beyond.

As of end July 2020, at the time of writing this, COVID-19 pandemic is still ongoing. As new technologies, measures and situations develop one after another, it is difficult to describe and assess what is still working. At a later date, new technologies may find solutions, or policies may change course. However, to facilitate evaluations by future generations, it is necessary to continuously communicate in real time and scrutinize the cases and evidences based on assessments made under both clear and unclear circumstances.

Rather than focusing on a single app or service, this special feature looks at the impact of COVID-19 in the context of the larger trend of data and AI ethics and governance discussions in recent years. Therefore, based on past trends, data and AI governance experts from around the world summarized the issues related to data, information technology, and AI technology during the COVID-19 pandemic from a medium to long-term perspective. While there is a growing consensus on international guidelines for data and AI technology, there is also a need to look at regional differences in culture, customs, and institutions across Europe, the Americas, Africa, and Asia. For this reason, this special issue focuses on Asia, particularly China, South Korea, Singapore, and Japan, where the infection spread first emerged.

“Ethics and Governance Perspectives to Fight Against Catastrophic Risks: From COVID-19 to Long-term Safety Issues of Artificial General Intelligence,” an article by Yi Zeng and his colleagues in China reveals how AI is used in various situations such as CT image recognition, drug discovery, and tracking apps as a countermeasure against COVID-19. In particular, the health code system for conducting contact tracing poses a problem in terms of a tradeoff between privacy and public health. Although the health code system is now mandatory, the article calls for regulations not only in technology but also in the use of AI and cooperation among related ministries and agencies, such as the need to reacquire consent for unintended use of personal information. Furthermore, the COVID-19 pandemic has proven the close link between humans and the environment. Learning from this lesson is important not only for future pandemic countermeasures but also for responding to technological developments and risks that focus on Artificial General Intelligence (AGI).

In the article “Harnessing Technology to Tackle COVID-19: Lessons from Korea” authors Sangchul Park and Yong Lim of South Korea point out how the nation successfully tamed the first wave of COVID-19 with the help of its IT infrastructure. Like Israel, South Korea introduced a centralized contact tracing system, but it was able to proceed under a legal framework put in to place following its prior encounter with the MERS outbreak. However, new challenges emerged, including privacy concerns; a survey revealed that the disclosure of personal epidemiological information for public health protection was of particular concern. The article enumerates Korea’s response to such challenges, which includes the introduction of anonymous testing, and the moderation of information publicly disclosed in consideration of its impact on individuals and businesses. The article points out that while technology can play an integral role in tackling public crises such as a global pandemic, it is equally important to carefully monitor secondary and tertiary effects of the use of technology, so as to ensure that vulnerable groups within society are not adversely impacted.

Similarly, "Singapore and COVID-19 Control — a Tale of Two Cities?" by Mark Findlay of Singapore brings to the fore the harsh environment of foreign workers and their living conditions, considered as a hotbed of the second wave of COVID -19, and also viewed as a social problem. Voluntary contact tracing apps using Bluetooth and access control systems using QR codes were introduced early to curb the first wave in the country. However, there is a limit to what can be done with technology alone, and only human intervention can explain, communicate, ventilate, and isolate contacts. Therefore, it is necessary to not just examine the technology but also understand the purpose for which data and technology are used, and how data are collected and used in a consistent manner among countries and organizations. The article underlines the importance of risk assessment and risk minimization in dealing with foreign workers, and reveals that the pandemic highlights structural discrimination already existent in society.

Lastly, the author overviews the present state of data, AI and COVID-19 in Japan entitled "Challenges of AI and Data Utilization and Governance in Japan Emerging from COVID-19 Response." The concept of Society 5.0, a human-centered society that simultaneously achieves economic development and the resolution of social issues, has been established in Japan through a system that integrates cyberspace and physical space. During the COVID-19 pandemic, data utilization among the government, private companies, medical institutions and consumers was promoted in some cases. However, it was also revealed that the situation is far from AI utilization, with difficulties even in sharing real-time data among various stakeholders including the government, local governments, and medical institutions. This is critical from a governance perspective in promoting the use of data and AI, and shows an urgent need to design systems and build consensus with relevant stakeholders in consideration of both protecting privacy and security, and ensuring fairness, transparency, and accountability.

The COVID-19 pandemic addresses key values for considering AI governance, such as human rights, fairness, and public safety. Given the current situation in which measures are taken in accordance with each country's systems, cultures, and experience, responses against COVID-19 can serve as a mirror reflecting our current society and values. It is expected that this special issue will be serve as a stimulus for discussions and thoughts on the matter not just during COVID-19 times but also beyond.

This report is the original English version of a special issue published by Information Processing Society of Japan (IPCJ) magazine, Vol.61, No.10 (Oct. 2020). This report was supported by Toyota Foundation Grant Number D18-ST-0008.

This report is based on a collaborative research of the following institutions:

- Technology Governance Policy Research Unit, Institute for Future Initiative, The University of Tokyo
- Centre for AI and Data Governance, Law School, Singapore Management University
- SNU AI Policy Initiative, Seoul National University
- Research Center for AI Ethics and Sustainable Development, Beijing Academy of Artificial Intelligence

CHINA

Ethics and Governance Perspectives to Fight Against Catastrophic Risks:

From COVID-19 to Long-term Safety Issues of Artificial General Intelligence

Yi Zeng, Kang Sun, Enmeng Lu

1. AI Ethics, Governance and Practices in Fighting Against COVID-19

Currently, the lockdown in Beijing has been ended, and we just recovered from the reappearance of COVID-19 cases starting from June 11th. We are still very positive that we humankind will definitely win to get over COVID-19. Although definitely not designed for it, AI/Data Analytics have been widely used to fight against COVID-19. In the history of AI, we seldom invent and develop a type of AI system just for a period, and has already decided to end its use after this special time. The use of AI to fight against COVID-19 will be a very special chapter in the history on the development and governance of AI.

We may face different catastrophic risks during the development of the human society, and we need to learn from each of them and help to avoid or at least to reduce the risks, if possible. Artificial General Intelligence (AGI) aims at building intelligent systems that can achieve human intelligence from every aspect of cognitive function that human has. They could be designed truly beneficial for the future of the society, while there could also be catastrophic risks to realize AGI without strategic preparations on potential long-term negative side effects. We will also discuss what we can learn from COVID-19 to avoid or reduce potential risks from AGI.

2. The use of AI to Fight Against COVID-19: Technical advancements, Ethical Risks, and Governance

2-1 Overview of AI usage to COVID-19

In the context of discussions related to COVID-19, Artificial Intelligence (AI), including big data analytics, knowledge representation and reasoning, pattern recognition, automated decision making, etc. has been used since the beginning of the outbreak. Until now, AI has been used for COVID-19 Spread Prediction, Potential virus hosts prediction based on gene sequence analysis, SARS-CoV-2 structure prediction, subtypes and variations recognition, automated CT image recognition, Voice Recognition for Detecting COVID-19, Virus detection, automated dialogue systems along with robots, Drug Discovery, and Automated health condition surveillance. More concrete examples and related technical discussions can be found in other publications[1]. In this paper, we focus on introducing technical and ethical challenges underlying each efforts.

Deep Neural Networks have been used for automated CT image recognition, even voice recognition to detect COVID-19. For example, by the end of February, Alibaba Damo Academy has conducted over 30,000 CT imaging diagnosis as suspected COVID-19 cases with 97% accuracy, and each case only need 20 seconds to test. Nevertheless, hidden layers in the multi-layered architecture have problems on explainability and transparency, which may lead to unreliable classification results. For example, for skin cancer identification, deep neural network will classify a normal skin image as with skin cancer even with a specific degree of adversarial rotation to the original image[2]. Similar risks may exists for COVID-19 CT image recognition.

Knowledge representation and reasoning has been widely used in drug screening and discovery, and automated dialogue systems along with robots for COVID-19 related services. For example, in China, several hospitals use some robots 24-hours a day for drug distribution, food and household goods delivery, treatment to help fight COVID-19. Baidu released an intelligent out-call platform, with 1 million calls to gather statistics, and make announcements for local communities and special groups who need extra care in Beijing, Xi(an, and Shanghai. The risk in here include but not limited to the quality of the medical knowledge related to drugs, and treatment. If the knowledge and inference rules are not strictly validated and conducted for consistency checking, conclusions and answers derived from the knowledge base and associated reasoning services will be not trustworthy.

Automated surveillance has been augmented in many ways to fight against COVID-19 in terms of finding and controlling potential risks. In the beginning of the pandemics, combined with facial recognition, automated temperature monitoring and tracking applications have been deployed in subways, train stations, airports, and social service centers to identify and track people with high temperatures, and to assist with necessary actions (Now relevant infrastructure has been replaced by health code (will be explained in Section 2.2) plus temperature monitoring). They could be of great help to assist screening (e.g. the version from Megvii could test 300 persons in a minute, and the version from SenseTimes can identify those who are with masks).

[1] Yi Zeng, Kang Sun. Fighting COVID-19 with AI: efforts and lessons from China. Global Times, March 7th. https://www.globaltimes.cn/content/1181846.shtml

[2] Finlayson, S. G., Bowers, J. D., Ito, J., Zittrain, J. L., Beam, A. L., & Kohane, I. S. (2019). Adversarial attacks on medical machine learning. Science, 363(6433), 1287–1289.

2-2 Health code system

Health code serves as the most important infrastructure to support the public health emergency management during the pandemics in China. Contact tracing for the health code is mainly based on GPS, and associated information from public transportations as well as other location based services. Related information for health code is mainly with centralized storage by different local governments, and similar strategy has been adopted by South Korea, New Zealand, Russia, India, etc[3,4]. Another approach is mainly based on Bluetooth, and are with centralized storage in Australia, Singapore, France, etc., and with decentralized storage in Italy, Germany, Japan, UK, Switzerland, Canada, etc[5,6].

The health code infrastructure and information collected for it is broader compared to other contact tracing apps. This is rooted from the differences on the design philosophy that various contact tracing apps hold. Firstly, the China health code asks more personal information to ensure its authenticity. It requires facial recognition for using it for the first time, and national ID information has to be provided. Hence, the phone number, real time facial information as well as national ID confirms it is really the owner of the cell phone using it. While for the other types of apps, it seems that without these information to some extend keep the privacy of users in a better way, but it will be very hard to confirm the real users of the cell phone. Secondly, China health code keeps mandatory so that the safety of life is put in the first place. Compared to voluntary in some other countries, for the one who has a smart phone, no one was left out of the public health emergency management system in China. The reason is that health code is widely used in China for managing human mobility, going back to work and to school. In China, the traditional philosophy of the self is based on the concept of "relational self", where "self" is part of a community, culture, and society. And the relations are important perspective to reflect the "self". Hence, access to personal private information by the public health crisis emergency management systems (as long as the systems are trustworthy) is designed to be doable, while voluntary participation is not acceptable, because the one who may not want to participate could be a potential risk to the safety of other people around. Thirdly, it can be observed that the health code system in China put effectiveness in the first place, with prerequisites of ensuring the security of private information.

In China, there are also local deployment of bluetooth based contact tracing services that support voluntary participation, such as the Blue Bubble COVID-19 tracing system, developed by Beijing Academy of Artificial Intelligence and Peking University, which has just released and deployed in some places in Beijing.

[3] Patrick Howell O'Neill, Tate Ryan-Mosley, Bobbie Johnson. A flood of coronavirus apps are tracking us. Now it's time to keep track of them. MIT Technology Review. May 7, 2020.

[4] Ethics and the Use of AI-based Tracing Tools to Manage the COVID-19 Pandemic. Institute for Ethics in Artificial Intelligence. Technical University of Munich, 2020.

[5] Patrick Howell O'Neill, Tate Ryan-Mosley, Bobbie Johnson. A flood of coronavirus apps are tracking us. Now it's time to keep track of them. MIT Technology Review. May 7, 2020.

[6] Ethics and the Use of AI-based Tracing Tools to Manage the COVID-19 Pandemic. Institute for Ethics in Artificial Intelligence. Technical University of Munich, 2020.

2-3 Social, Ethical, and Legal concerns, and responses to Data Governance

The stakeholders of traditional healthcare systems have been greatly expanded from patients and doctors to AI service providers (mainly companies), different levels of governments, community and block staffs, gate keepers and volunteers, at least in China public health crisis emergency management systems. They are working very hard to reduce infections and keep providing necessary feedbacks to higher levels of organizations for decision making, which are very valuable contributions to fight against the pandemics. Nevertheless, clearly not all of them are behaving according to the current policies to protect personal data and ensure human agency, which may lead to ethical risks on privacy, bias, safety, and accountability, etc.

In February, personal information on Wuhan residents was posted online and in WeChat groups. It caused biases, isolation, and have negative effects for personal reputations. On February 1st, the network police branch of Linyi City Public Security Bureau in Shanxi Province announced that a local man had distributed "close contacts list" with 35 people (the list of names, identity card numbers, home addresses and other personal information) in the WeChat group, has been administratively detained in accordance with the law. Similarly, the deputy director of health bureau of Yiyang district, Hunan province, was investigated due to leaking the privacy of COVID-19 patients. Although more personal information might need to be collected due to biological and social safety reasons during this period, access control and release of the information need to be regulated accordingly.

Policies that promote and regulate the beneficial use of AI to fight against COVID-19 are necessary, such as the efforts for promoting the beneficial use of AI for COVID-19 from the Ministry of Science and Technology China. And to protect the private information during the pandemics, a multi ministry coordination framework is established. Ministry of Transport China issued the "Emergency Notice of the Ministry of Transport on the Coordination of COVID-19 Prevention and Control and Transport Security" in January 30th, 2020, which states: "To strictly protect personal privacy and personal information security in accordance with the law, only to satisfy the need for COVID-19 prevention and control, to health and other closely related departments. No other institutions, organizations or individuals may disclose relevant information or distribute it on the Internet without authorization." On March 2nd, 2020, the Ministry of Civil Affairs, PRC Cyberspace Administration of China, Ministry of Industry and Information Technology, National Health Commission jointly issued the "Information Construction and Application Guidelines for Community Prevention and Control of COVID-19 Outbreak, First Edition", which states:

"prevention and control of information products (services) are needed due to the requirements of the COVID-19 prevention and control work. The need to collect information of community residents, should be clearly prompted to the community residents and obtain consent, clearly used for the prevention and control of the virus, for other purposes, must re-obtain the consent of the community residents themselves".

2-4 Privacy Protection for Public Health Management

Protecting privacy is not something that can be postponed during pandemics. And it can be properly protected if effective regulation and security infrastructures are properly taken. By the end of May 31st this year, 216 Countries, areas or territories are with confirmed COVID-19 Cases, based on WHO data as of, 08:00 GMT+8. Among which, at least 63 Countries and regions (no more than 1/3) has published Privacy/Data/AI Governance related policies[7]. In the case for China, most of the health code related data are maintained by reginal big data centers in different cities, while the technology and the infrastructures are provided by companies such as Alibaba and Tencent. Hence, multiple types of stakeholders need to take different responsibilities to ensure the safety and security of personal information. Due to the fact that even gate keepers and volunteers may have access to some private information, privacy protection policies need to be getting aware of by all the stakeholders in the public health crisis emergent management systems.

There was a proposal from Hangzhou Ministry of Healthcare on extending the use of the health code after the pandemics, and the health code as well as related services could record private information on daily physical exercise, drinking, smoking, or even sleep duration details and the data are designed to be summarized and provided to at least organization level. A flood of people criticized the design online in a very consistent way, saying "The health code should only be for COVID-19 period!", or "Clear division should be made to personal health and public health. The health code is designed to be shown to others, but my personal health report is not". From the policy level, this idea has already been with violation with the "Information Construction and Application Guidelines for Community Prevention and Control of COVID-19 Outbreak, First Edition" released by the PRC cyberspace administration of China and other ministries, since it clearly stated that "for other purposes, must reobtain the consent of the community residents themselves". It was later reported that it is a "design idea", and currently they do not have plans to launch. It is not that having personal healthcare management services are not good. The key point is that extending the use of private data acquired to fight against COVID-19 need to reobtain the consent.

[7] COVID-19 Resources Library, Global Privacy Assembly. 2020. https://globalprivacyassembly.org/covid19/covid19-resources/

In a recent survey on "Facial Recognition and Public Health" based on Chinese users[8], it has been observed that: (1) The respondents generally appreciate the benefits of installing facial recognition in areas with public (health) security concerns. (2) The respondents are concerned about their privacy related to the uses of facial recognition despite of COVID-19 pandemics, which means that they did not reduce the expectation to protect their privacy by the governments, private sectors, community and block staffs, etc. (3) The COVID-19 public health crisis increased the acceptability of facial recognition among the general public. (4) The respondents hope the application of facial recognition can be reduced when the pandemic ends. They believe facial data collected at this special time should be deleted afterwards, and that unnecessary facial recognition applications should be eliminated. (5) Some of the respondents are not sure whether they support the reduction of facial recognition applications related to public health crises when the pandemic ends, which shows their concern over the recurrence of such public health crises and similar potential crises. This also gives weight to appreciating the potential of such technology to be prepared for future emergencies. Other respondents express reservations in terms of reducing facial recognition usage when the emergency ends, which highlights the necessity to establish a public health crisis precautionary and defense system driven by technology in order to prepare for any recurrence[9]. This consideration has been validated its necessity and effectiveness during the recent reappearance of COVID-19 cases in Beijing starting from June 11th, 2020.

The use of contact tracing apps world wide is based on the fact that users have to be with a cellphone or smart device with Bluetooth, GPS, etc. While at least in China, around 76.86% of the whole population is with at least one cellphone, which means that more than 1/5 of the people do not have ways to have a health code. This is also true world wide. It is reportedly that approximately 30% of the people in the world do not have a cellphone. In order to enable the beneficial use of AI to all, we need to collectively reach the state of leaving no one behind for digital communications.

3. Yet Another Potential Catastrophic Risk: Long-term Safety Issues of Artificial General Intelligence

We should definitely learn from and share each other's experiences. This is not easy when people are with different cultures, but it is exactly why it is important to see why people and countries with different cultures have different approaches to deal with this crisis. What can we learn to complement with each other is the real key to build the shared future for humanity.

Pandemics prediction system at large-scale should be strengthened, with even more transparent data contributions from different countries and regions.

[8] Yi Zeng, Enmeng Lu, Kang Sun, Samuel Curtis. Facial Recognition and Public Heath. Technical Report. Beijing Academy of Artificial Intelligence, 2020.

[9] Yi Zeng, Enmeng Lu, Kang Sun, Samuel Curtis. Facial Recognition and Public Heath. Technical Report. Beijing Academy of Artificial Intelligence, 2020.

Surveillance systems and services related to healthcare are widely deployed for this COVID-19 pandemics. We need to learn and decide what can be left as possible infrastructures to support avoiding future pandemics, but cannot be too much, which may lead to negative side effect for human agency, privacy, and human rights in general.

Lack of strategic design and long-term research for preventing and fighting against potential catastrophic risks is a lesson we should learn from COVID-19 pandemics, but this definitely also applies to long-term AI. It is still not clear when we are going to have AGI and Supperintelligence, but it is quite clear that no matter which way we are going to realize them, there could be various different potential catastrophic risks. As Norbert Wiener stated more than 60 years ago, "we had better be quite sure that the purpose put into the machine is the purpose which we really desire". We might be able to build an AI with hundreds of cognitive functions and solve unseen problems with self organizations based on simpler building blocks, and we might bring quasi-members to our society. But it is also possible that the AI got reflexive thinking to ask why do I have to obey what you said, and why do I have to hold your values while it is already hard for human to agree on each other. We want to humanize AI so that it would be easier for us to welcome them as quasi-members, but we are also not sure whether the future AGI will learn to be with discrimination and hostility. We definitely need strategic design and long-term research for reducing the risks and avoiding the catastrophic ones on our way to AGI and Supperintelligence. In addition, we should have a very well coordinated global team to ensure beneficial AGI and superintelligence, taking challenges from various technical and cultural perspectives, sharing, and bridging the efforts for the whole societies.

During this pandemics, we should have learned that different countries and regions are so closely interconnected with each other, and no one will going to win if we left someone behind. Similar challenges may also exist when possibly not so well designed AGI and superintelligence become part of the society. We should also have learned the fact that humankind is very vulnerable, and we are tightly interconnected not only with each other, but also with the environment, and we are only a portion of the ecosystem. Continuous efforts should be made to make sure our connections to each other and the environment are in positive and sustainable ways. During but not limited to pandemics, we should not blame or even hurt each other in any way, but to hold hands tightly and bridge our efforts together for the symbiotic societies.

Yi Zeng

Email: yi.zeng@ia.ac.cn
Bio: Professor and Deputy Director at Research Center for Brain-inspired Intelligence, Institute of Automation, Chinese Academy of Sciences, and Founding Director at Research Center for AI Ethics and Sustainable Development, Beijing Academy of Artificial Intelligence in China, a member of the National Governance Committee on the New Generation AI, China, and an expert of the UNESCO Ad Hoc Expert Group on AI Ethics.

Kang Sun

Email: keitht@126.com
Bio: Kang Sun is a visiting researcher at Research Center for Brain-inspired Intelligence, Institute of Automation, Chinese Academy of Sciences.

Enmeng Lu

Email: enmeng.lu@ia.ac.cn
Bio: Enmeng Lu is a research engineer at Research Center for Brain-inspired Intelligence, Institute of Automation, Chinese Academy of Sciences.

SOUTH KOREA

Harnessing technology to tackle COVID-19: Lessons from Korea

Sangchul Park, Yong Lim

1. Korea Responds to COVID-19[10]

Korea's first case of COVID-19 was reported on January 20, 2020. By the end of February, the nation was witnessing an outbreak that was threatening to spiral out of control. Korea, however, had already put in to place a legal framework for IT-based contact tracing following its bruising encounter with the Middle East Respiratory Syndrome (hereinafter, "MERS") in 2015. This enabled Korea to swiftly mount an aggressive trace, test, and treat strategy instead of having to resort to more extreme measures such as shelter-in-home and lockdowns that would significantly burden the economy. Under legal authorization, the nation's IT infrastructure was mobilized to support the healthcare professionals' and epidemiological investigators' efforts to flatten the curve of newly confirmed cases and deaths, a goal achieved by mid-March. While the aforementioned legal framework provided the necessary means to launch an IT-based response to COVID-19, new challenges arose in the process such as the need to protect the privacy of those infected and/or exposed while maintaining the effectiveness of the response. This article provides an overview of how Korea harnessed the power of technology to confront COVID-19, and discusses some of the issues related to the governance of data and technology that were raised during Korea's recent experience.

2. The Role of Technology in Korea's Response to COVID-19

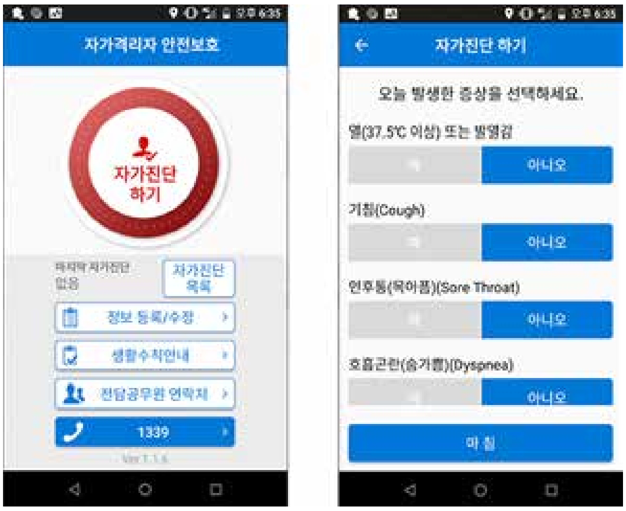
The following is a summary of the major technological means used by Korean authorities to tackle the pandemic.

2-1 GPS Tracking for Quarantine Measures

Upon authority provided under the Contagious Disease Prevention and Control Act (hereinafter "CDPCA"), those proximately contacted by confirmed cases (starting from February 23), as well as all persons arriving from foreign countries

[10] This article's description of Korea's IT-based response to the COVID-19 pandemic and its implications is in part based on Sangchul Park, Gina J. Choi & Haksoo Ko, Information Technology-Based Tracing Strategy in Response to COVID-19 in South Korea — Privacy Controversies, 323(21) JAMA 2129 (2020) (quotations omitted).

(expanded to all countries as of April 1, 2020) are currently being quarantined for 14 days. To monitor compliance, those quarantined are required to install and run a mobile app called the 'Self-Quarantine Safety Protection App' developed by the Ministry of the Interior and Safety. The app enables officials at competent local governments to track GPS data from smart devices held by those quarantined on a real-time basis, through the Geographic Information System, to check whether they have remained in their place of quarantine.



오늘 발생한 증상을 선택하세요.

열(37.5℃ 이상) 또는 발열감

기침(Cough)

인후통(목아픔)(Sore Throat)

호흡곤란(숨가쁨)(Dyspnea)

<Image 1> User interface of the Self-Quarantine App[11]

The app requests those quarantined to report symptoms, if any, twice a day. To comply with the consent requirements for the collection and use of personal location data under Korea's Act on the Protection and Use of Location Information, the app requests an installer to click on the consent button. Since installing the app and providing consent allows one to avoid the inconvenience of being manually monitored by the quarantine authorities or possible refusal of entry into the country, most of those subject to quarantine have chosen to use the app.

2-2 Automated Contact Tracing

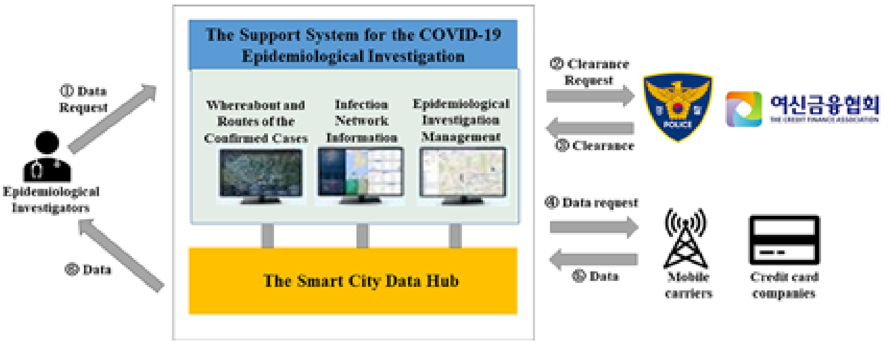
Manual contact tracing by epidemiological investigators naturally has limits that inhibit the timely detection and quarantine of those suspected of infection. In response, several automated contact tracing models based on geolocation data have been devised. However, there is a global divide as to which specific technology to deploy. Japan, the majority of the EU members[12], Singapore, Australia, and a few U.S. states have chosen decentralized, user-centered, or 'privacy-preserving' proximity tracing techniques based on Bluetooth Low Energy. This includes the partially centralized approach such as PEPP-PT (adopted by France and being tested by U.K.) and BlueTrace (developed by Singapore and adopted by Australia), and the fully decentralized approach such as DP3T (adopted by Austria) and Apple-Google's Exposure Notification API (adopted by Japan and the majority

[11] Google Play Store/ Ministry of the Interior and Safety, Self-Quarantine Safety Protection App, https://play.google.com/store/apps/details?id=kr.go.safekorea.sqsm&hl=ko (Accessed July 28, 2020, in Korean)

[12] Exceptions include Iceland and Norway (prior to its data protection agency's ban of GPS tracking on June 12, 2020) which, respectively, is deploying or had deployed a GPS tracking app.

of the EU members). Israel and Korea, on the other hand, have taken centralized network-based tracking approaches based on geolocation data collected from mobile carriers and other data. Israel reportedly resorted to its emergency powers to redirect its intelligence agency's counterterrorism monitoring program for contact tracing, which its Supreme Court later held to be unlawful unless the practice is brought under legislation. As explained below, Korea acted under legal authority pursuant to the CDCPA to redirect its smart city data hub system for the same purpose.

A major hurdle to implementing such a centralized network-based approach in Korea was the Personal Information Protection Act (hereinafter, "PIPA") and other data protection laws, which require prior consent from the data subject or a court warrant for the collection and use of personal data. However, the previous MERS outbreak had shown the need for effective contract tracing and prompted Korea to amend the CDPCA that allowed the overriding of such consent requirements under certain circumstances in the event of an outbreak. Following the amendments, public agencies including the Korea Centers for Disease Control and Prevention (hereinafter "KCDC") and the Ministry of Health and Welfare could, at the outbreak of a serious infectious disease, collect the following categories of data that pertain to confirmed cases or those contacted by them without an issued warrant: location data; personal identification data; medical and prescription records; immigration records; card transaction data for credit, debit, and prepaid cards; transit pass records for public transportation; and closed-circuit television (hereinafter, "CCTV") footage. The KCDC could further share this data with other government and national health insurance agencies, health care professionals and their associations, and also transfer certain information to national health insurance information and other designated systems, thereby ensuring a coordinated and comprehensive tracking and treatment system to cope with the outbreak.


① Data Request
Epidemiological Investigators
⑥ Data
The Support System for the COVID-19 Epidemiological Investigation
Whereabout and Routes of the Confirmed Cases
Infection Network Information
Epidemiological Investigation Management
The Smart City Data Hub
② Clearance Request
③ Clearance
POLICE
여신금융협회
THE CREDIT FINANCE ASSOCIATION
④ Data request
⑤ Data
Mobile carriers
Credit card companies

<Image 2> Support System for the COVID-19 Epidemiological Investigation[13]

Based on this mandate and authority, the Korean government launched the Support System for the COVID-19 Epidemiological Investigation (hereinafter, "Support System") on March 26, 2020, which was swiftly remodeled from the

[13] Ministry of Land, Infrastructure, and Transport ("MOLIT"), MOLIT, MSIT, and KCDC Launch the COVID 19 Data Platform (March 26, 2020), http://www.molit.go.kr/english/USR/BORD0201/m_28286/DTL.jsp?id=eng_mltm_new&mode=view&idx=2931.

smart city data hub system developed by several municipal governments. The Support System collects requisite data pertaining to confirmed cases and those contacted, including base station data and credit card transaction data, from mobile carriers and credit card companies under clearances from the police and the Credit Finance Association, and delivers them to epidemiological investigators on a near real-time basis[14].

In addition to the Support System, epidemiological investigators at municipal or local governments are, upon request, given access to the Drug Utilization Review by the KCDC. In June 2020, Korea further launched a Japan-invented QR code-based electronic visitors' booking system to track visitors of designated high-risk premises such as nightclubs, with the help of leading local internet companies.

2-3 Public Disclosure of the Routes of Confirmed Cases

Pursuant to the CDPCA, in the event of an outbreak of a serious infectious disease, the KCDC must promptly make the following information publicly available on the internet or through a press release: the routes and means of transportation of the confirmed cases; the medical institutions that treated the confirmed cases; and the health status of close contacts with the confirmed cases. The disclosed information is also sent to mobile phones held by nearby residents to alert them of possible exposure and risks via an emergency mobile alert.

3. Tech Governance Issues in the COVID-19 Era

3-1 Technology Enabled Centralized Contact Tracing

An early response is critical to containing the spread of highly infectious diseases like COVID-19. And the effectiveness of such a response in turn relies on the prompt collection and sharing of data about confirmed cases and close contacts among medical professionals and the wider public as appropriate. But, human (manual) epidemiological tracing by investigators based on interviews with confirmed cases and contacts has proven to have limitations not only in terms of the time required but also its vulnerability to faulty memory or deception on the part of interviewees. Meanwhile, human surveillance of quarantined persons is often costly, ineffective, and in many cases inevitably intrusive. In response to the rapid spread of COVID-19, Korea chose to integrate such human efforts with information technology and data analytics. For example, the prompt profiling of geolocation data has been a crucial enabling factor in Korea's trace, test, and treat strategy. The near real-time Support System, which makes use of smart city technology as well as machine learning models, allowed authorities to efficiently allocate valuable resources in the face of constraints, such as directing epidemiological investigators to focus their efforts on promptly tracing contacts to identify and quarantine potential cases in a timely manner.

[14] Ibid.

Some have questioned whether a centralized contact tracing model like Korea might be unnecessarily intrusive and as such unadaptable for democratic and free societies. This argument might have merit if Korea's approach had ignored due process and exceeded legal boundaries, while other more decentralized models, such as the Bluetooth-based approach, provided a valid alternative in terms of epidemiological efficacy.

In fact, the decentralized model comes with certain shortcomings that have yet to be resolved. First, a decentralized tracing app needs to attain a certain penetration rate, i.e., the proportion of active users of the mobile app to the population — often set at 60% — for proximity tracing to function properly (so called "digital herd immunity"). However, this threshold is not easy to attain, with one important constraint being the non-insignificant portion of the population that does not use smart devices. Secondly, Bluetooth-based proximity tracing may not work properly in crowded areas that are in fact prone to explosive outbreaks of infectious diseases such as COVID-19. Thirdly, decentralized models generally do not allow for human-in-the-loop based verification and thus are prone to excessively high false positives. Fourthly, iOS does not allow third-party apps from broadcasting Bluetooth signals in the background, unless the Apple-Google API is deployed as in Japan's COCOA app. Lastly and perhaps more fundamentally, the decentralized approach is not that different from the manual investigation method to the extent that it has to resort to good-faith cooperation from confirmed cases, and thus exhibits the same problems. This is not to argue that a centralized model would always be preferable, but rather that it may have certain advantages over current decentralized alternatives, such as immediate availability (unaffected by the penetration rate), effective response to mass infection, no compatibility concerns, and most importantly, impactful contribution to epidemiological investigations.

Meanwhile, loosely referring to "Confucian" values or "authoritarian" tendencies as the background of the centralized approach ignores the fact that Korean society, after achieving democratization, has exhibited strong preferences for the privacy and other rights of data subjects, as demonstrated through its highly stringent data protection and privacy law regime. Some point to Korea's relatively small geographic size as an advantage for epidemiological responses, but the nation's extremely high population density in fact creates challenges to successfully implementing an effective response to a pandemic.

At the same time, merely crediting Korea's use of technology for the nation's initial success in flattening the curve also overlooks a critical societal factor that contributed to such an outcome — a broad acceptance of the need to retain flexibility in terms of trade-offs between privacy and health policy. Stung from their prior experience with the MERS outbreak, citizens exhibited such flexibility by willingly cooperating with authorities in both the human and technological collection and sharing of epidemiological information (e.g., geolocation data), reasoning that health and economic risks could be further exacerbated if the trace, test, and treat strategy failed. Such cooperation at the societal level, buttressed with an IT-based strategy guided by an established legal regime, allowed Korea to mount an effective campaign against the disease.

Compared to the Korean government's active role in utilizing technology to cope with the COVID-19 pandemic, public-private collaboration based on the sharing of public data and the use of open APIs in Korea has somewhat lagged Taiwan and other jurisdictions. There have been recent cases of meaningful contributions from the private sector, however, such as a collaborative dataset sourced from public disclosures by the KCDC, which is being actively used for visualizing cases and training machine learning models[15].

3-2 Public Disclosure of the Route of Confirmed Cases

Unlike contact tracing itself, which was generally accepted as a necessary trade-off between privacy and public health in face of a pandemic (although several non-governmental organizations have mounted constitutional law challenges), the public disclosure of the routes of confirmed cases quickly became controversial due to privacy concerns. Such public disclosures were in fact another policy response to the prior MERS outbreak which showed that a lack of transparency could significantly impede an effective response to an outbreak. While the disclosures did not include the identity, including the names, of the confirmed cases, it turned out to be possible to publicly profile and unveil embarrassing personal details, and in some cases even re-identify specific persons. The uneven scope and granularity of disclosures among the KCDC and the numerous municipal and local authorities also caused confusion and eroded public trust towards the nation's privacy law regime. Concerns were not limited to the invasion of privacy. Private businesses, such as restaurants and shops, that were identified as part of the routes often experienced abrupt and sustained loss of business.

These concerns were encapsulated in the National Human Rights Commission (hereinafter, "NHRC")'s recommendation of March 9, 2020[16]. The NHRC expressed concern about unwanted and excessive privacy invasion and secondary damages such as public disdain or stigma, citing a recent survey by Seoul National University's Graduate School of Public Health showing that the public was even more fearful of the resulting privacy invasion and stigma stemming from an infection than the associated health risks itself. The NHRC noted that excessive public disclosure could also undermine public health efforts by dissuading those suspected of infection from voluntarily reporting and/or testing for fear

[15] MOLIT, Online Q&A for the Support System for the COVID-19 Epidemiological Investigation (April 10, 2020), http://www.molit.go.kr/USR/NEWS/m_71/dtl.jsp?id=95083773 (in Korean).

[16] NHRC, Statement concerning the Excessive Disclosure of Private Information Pertaining to Confirmed COVID-19 Cases (March 9, 2020), https://www.humanrights.go.kr/site/program/board/basicboard/view?currentpage=2&menuid=001004002001&pagesize=10&boardtypeid=24&boardid=7605121 (in Korean).

of privacy intrusions. The NHRC further recommended that route (visited premises) disclosures be made in an aggregate manner, rather than disclosing the time and place of visit individually for each confirmed case, and concomitantly providing information on disinfection and other infection controls that had been implemented at the visited premises.

In response to the NHRC's recommendations, the KCDC issued its first guidelines regarding public disclosure to municipal and local governments on March 14, 2020, which limited the scope and detail of the information to be publicly disclosed. Specifically, the KCDC (i) limited the period of route disclosure from one day prior to the first occurrence of symptoms to the date of isolation, (ii) limited the scope of visited places and means of transportation to those spatially and temporally proximate enough to raise concerns of contagion, considering symptom, duration of visit, status of contact, timing, and whether facial masks were worn, and (iii) banned the disclosure of detailed home addresses and names of workplaces. On April 12, the KCDC further revised the guidelines so that (i) information on routes are taken down 14 days after the confirmed case's last contact with another person, (ii) information on "completion of disinfection" is disclosed for relevant places along the disclosed routes, and (iii) the period of route disclosure starts from two days prior to the first occurrence of symptoms[17]. In light of the rapid dissemination of the disclosed information via blogs and social network sites, data protection agencies are actively sending takedown notices to online service providers to ensure that such content are taken down following the lapse of the 14 day period.

In May 2020, a spate of confirmed cases arose at a gay nightlife district in Itaewon. Concerned that those who had visited the relevant premises might be deterred from voluntarily reporting and testing for fear of forced outing and/or being ostracized, the Seoul Metropolitan government initiated anonymous testing where individuals were only required to leave their phone number starting from May 11. The KCDC expanded such anonymous testing throughout the whole country on May 13, while deleting the name of gay nightclubs from publicly disclosed routes.

The above evidences an ongoing process of trial and error in search of a more refined approach that better balances the imperative of saving lives with privacy and other social values during a pandemic. The urgency of the situation might demand the swift implementation of both public and private measures, hence the importance of continuously reviewing and revising measures so that they better preserve privacy while remaining effective. Rather than disclosing precise routes profiled for each confirmed case, the disclosure of aggregated route information has proven sufficient to achieve the intended objectives of such disclosures,

[17] KCDC, Guidance to Information Disclosure of Transit Routes of Confirmed Patients, etc. (April 12, 2020), http://www.cdc.go.kr/board.es?mid=a20507020000&bid=0019&act=view&list_no=367087 (in Korean).

namely transparency, information symmetry, public awareness, and the reduction of false information. As pointed out by the NHRC and demonstrated in the Itaewon case, this less intrusive alternative can also assist infection control efforts by encouraging voluntary reporting and testing. Assuming that disinfection can effectively address contagion after lapse of a reasonable time, the only benefit from identifying the relevant premises would be alerting other visitors and encouraging them to self-report and get tested. Therefore, if all visitors are in fact identifiable through contact tracing, the public disclosure of the type of business and the broader area of the location, rather than identifying the name of the specific business premise, should be sufficient for policy purposes.

The outbreak of COVID-19 has highlighted the need for Korea's privacy and data protection authorities to be ever more vigilant during public emergencies. In February, Korea undertook major reforms to its privacy and data protection laws which came into effect as of August 5, 2020. As a result of the amendments, Korea's data protection authority will be consolidated and vested in the Personal Information Protection Commission (hereinafter, "PIPC"), which will become an independent agency. This reform should allow the PIPC to engage in a more proactive role in balancing the rights of data subjects with public health goals and providing clearer guidance as to how to de-identify information for public disclosure.

4.Looking Ahead

As the COVID-19 outbreak continues its course, new societal challenges or existing ones that are being exacerbated by the pandemic such as the digital divide, are garnering more attention in Korea and elsewhere. Heightened concerns of ostracization or stigma directed to minority groups, the vulnerability of health and other essential workers that face constant exposure to infections, and children from underprivileged families that are ill equipped for remote learning are but a few examples. The Itaewon case mentioned above, has demonstrated the need for authorities to be prepared to promptly address concerns of prejudice against minorities. The same should be said regarding the acute health and economic disadvantages faced by the underprivileged during a pandemic. Yet the societal challenges in the post-COVID-19 era, with its trend towards remote work, education, and economic activity will likely call for more long-term and fundamental solutions. In this regard, the active use and application of AI and data analytics, as well as a robust ethical review concerning its governance, is expected to be critical in achieving the social reforms required to cope with the challenges of the present and coming future.

Sangchul Park

Email: mail@sangchul.com
Bio: Assistant Professor at Seoul National University, School of Law

Yong Lim

Email: yonglim@snu.ac.kr
Bio: Associate Professor at Seoul National University, School of Law. He is also the Co-Director of Seoul National University AI Policy Initiative.

SINGAPORE

Singapore and COVID-19 control – a tale of 2 cities?

Mark Findlay

1. Response to control the spread of COVID-19 in Singapor[18]

This brief review of controlling COVID-19 in Singapore has two purposes. First, it describes the largely technology-based approaches to reducing infections that have been instituted in Singapore since early 2020. Some of these approaches are novel, others are more tried and tested, and all work together in a holistic strategy for national health safety. The second intention is to explore how inadequate social risk prediction has led to large scale infection in a vulnerable social demographic and the consequences this has had for the control strategy evolving.

Nation state jurisdictions and private organisations, in differing forms and at different trajectories, are creating, instituting and maintaining various tactics to control the spread of COVID-19. Many of these involve the compromise of personal data and the restrictions of individual liberties. Principle among such strategies, are

1) Closing of national borders
2) Quarantining individuals and populations for varying periods of time, usually requiring that they remain in their places of residence and don't associate with others not living with them
3) 3) Restricting social association either through 'lockdown'regimes or social distancing conventions
4) 4) Restricting attendance at schools, places of worship, entertainment venues and other locations which conventionally attract large numbers of people in close proximity
5) Special restrictions placed on elderly citizens, the incarcerated and institutionalized groups
6) Virus screening and testing
7) Manual tracing of association and manual human tracing
8) Tracing and tracking through mobile-phone applications
9) Surveillance and toggle device personal identification
10) Safe entry requirements into designated businesses and services sites, with

[18] This brief review was assisted by the following working papers – 1) Findlay, Mark James and Remolina, Nydia, Regulating Personal Data Usage in COVID-19 Control Conditions (May 22, 2020). SMU Centre for AI & Data Governance Research Paper No. 2020/04. Available at SSRN: https://ssrn.com/abstract=3607706, 2) Findlay, Mark James and Loke, Jia Yuan and Remolina, Nydia and Tham, Benjamin, Ethics, AI, Mass Data and Pandemic Challenges: Responsible Data Use and Infrastructure Application for Surveillance and Pre-emptive Tracing Post-crisis (May 4, 2020). SMU Centre for AI & Data Governance Research Paper No. 2020/02. Available at SSRN: https://ssrn.com/abstract=3592283 or http://dx.doi.org/10.2139/ssrn.3592283
3) Findlay, Mark James and Seah, Josephine, Data Imperialism: Disrupting Secondary Data in Platform Economies Through Participatory Regulation (May 29, 2020). SMU Centre for AI & Data Governance Research Paper No. 2020/06. Available at SSRN: https://ssrn.com/abstract=3613562 or http://dx.doi.org/10.2139/ssrn.3613562
This research is supported by the National Research Foundation, Singapore under its Emerging Areas Research Projects (EARP) Funding Initiative. Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not reflect the views of National Research Foundation, Singapore.

temperature checking and personal detail recording.

These intrusions have been met with community reactions ranging from individual participation and compliance, to hostility and resistance. Popular discontent with these infringements has focused on challenges to personal data protection, as well as restrictions on freedom of movement and association. In Singapore, where there is no constitutional right to privacy and data protection legislation does not apply to the government sector, concern evidenced over social media has taken the form of confusion about the scope and reach of mobile applications rather than apprehension for privacy compromise or data abuse.

Social distancing has been required by the state through its 'circuit breaker' policy. This control regime, which is currently (as at June) undergoing a phased transition, applied to all residents in the country and involved periods of quarantine for designated individuals, special guidance for the protection of vulnerable groups and a general application of movement and association restrictions. The circuit breaker was accompanied by a vigorous commitment to mass testing and manual contact tracing.

Migrant construction workers living in dormitories have been subject to stricter confinement. Since the outbreak of virus infection in one of the main dormitory settlements in April, dormitories have been under total lockdown conditions progressively as virus infections have evidenced in different establishments. The policy of complete quarantine under conditions where safe distancing is unsuitable has produced large scale virus incubation, but contained the spread into the general community, which at this stage remains low.

This review does not critique individual control policies beyond examining their potential to exacerbate already-existing structural discrimination in Singapore society.

2. Singapore Case-study in COVID-19 Control

Singapore has adopted certain AI-assisted control measures against carriers and to protect the vulnerable. By 'AI-assisted' we mean here the use of either algorithm analysis or AI-enabled communication technologies. The following are some AI-assisted COVID-19 Control Strategies:

2-1 Stay-Home-Notice (SHN)

Prior to the Infectious Diseases (COVID-19 — Stay Orders) Regulations 2020, a 14-day SHN is issued to all travellers entering Singapore (inclusive of all Singaporeans, Permanent Residents, Long Term Pass holders and short-term visitors) and exhibiting fever and/or other symptoms of respiratory illness with a negative Covid-19 swab test from 13 March 2020. All travellers who refused to undergo the Covid-19 swab test when requested could be prosecuted and face penalties. From 20 March 2020, 2359h, tighter measures, in the form of a 14-day SHN were issued to all travellers entering Singapore. This notice was a major control strategy before Singapore closing its borders to foreign travellers, and it will form a continued control as these restrictions are incrementally lifted. The policy is both manual and AI-technology assisted (through smart phone applications and data harvesting).

Persons under a 14-day SHN must remain in their place of residence at all times, during the 14-day period. They may not leave their residence, even if it is to purchase food and essentials or to attend to important personal matters, save for circumstances whereby medical attention is required. Any person who is subjected to a 14-day SHN and leaves the place of accommodation specified in the SHN during the period specified in the SHN without reasonable excuse is guilty of an offence and shall be liable on conviction to a fine not exceeding $10,000 and to imprisonment for a term not exceeding 6 months or to both.

If a Singapore Permanent Resident, Long-Term Visit Pass holder, Dependent's Pass holder, or Student's Pass holder fails to comply with a 14-day SHN, his/her respective Re-Entry Permit or passes may be revoked, or the validity shortened. If a foreign employee issued with a work pass fails to comply with a 14-day SHN, his/her work pass may be revoked pursuant to s7 (4)(a) of the Employment of Foreign Manpower Act. If a full-time student attending a preschool, school or other educational institution in Singapore fails to comply with a 14-day SHN, the student may be subjected to disciplinary action, including suspension or dismissal. For foreign students, this may include the cancellation of your child's/ward's Student's Pass or Dependent's Pass.

The Ministry of Manpower (MOM) instituted mobile phone text prompt surveillance of SHN recipients. A notice on MOM's webpage prompts and guides the recipient to activate location services on his/her mobile phone. The web browser notifies the recipient that "[The webpage] wants to: Know your location". The recipient then accepts the request and the web browser sends the location of the mobile phone (determined by GPS) to MOM's webpage.

The "Privacy Statement" on the webpage provides as such: "The collected data would be retained for up to six months after the Government ceases the leave of absence (LOA/SHN) and any other related precautionary measures. Unless required for subsequent enforcement follow-up, the collected data would be destroyed once the retention period lapses. The collected data would not be used or shared for purposes other than for ensuring your compliance with the LOA/ SHN or precautionary measures."

In addition, the SHN recipient may be subject to home visits and/or are required once called by the Immigration and Checkpoints Authority (ICA) to take photos of their surroundings in order to verify their whereabouts at random timings. This is all carried out by manual labour.

At the end of May, MOM launched an app called the "FWMOMCare" mobile app. Workers should use the app to record their temperatures twice daily, and indicate if they have a cough, sore throat, runny nose, or shortness of breath. If the worker reports any symptoms, the app will prompt him to seek medical assistance. A doctor will also be alerted and will contact the worker within 30 minutes to provide a teleconsultation.

Also, to keep employers updated on the latest movements of their workers, MOM created a new "Government Facilities Listing" feature within the Online Foreign Worker Address Service (OFWAS). Employers can use this feature to check on the location of their infected workers who have been moved to other quarantine facilities by the COVID-19 Inter-Agency Task Force, of government.

2-2 TraceTogether App

TraceTogether is a mobile application developed by GovTech Singapore in collaboration with Singapore's Ministry of Health, which assists in contact tracing, if and when required. Downloading and activating TraceTogether is voluntary. That said, migrant workers who live or work in high risk areas are required to download, activate and maintain the latest version of the app. Presently the take-up rate for this app in Singapore is insufficient for the required population coverage to be met.

TraceTogether works by advertising a Temporary ID over Bluetooth Low Energy technology ("BLE"). When two devices (with TraceTogether installed and activated) are co-located within BLE range, they can detect each other and record this encounter in the local storage. These records will then be stored locally in the users' phones.

Assuming that a user of TraceTogether tests positive for Covid-19, users will be asked to share these records when contacted by the Ministry of Health as part of contact tracing investigations. This therefore facilitates (instead of relying on one's memory) and greatly speeds up the contact tracing process, which is crucial to limit the spread of the Virus. TraceTogether acts as a pre-emptive tracing method as it tracks the people a non-susceptible person comes into contact with in his/her daily activities.

TraceTogether does not access a user's phone contact list or address book, nor does it collect or use location data automatically. Obviously, the purpose of the app is as a locator, but that information is provided by the user. TraceTogether seeks to establish who may have been exposed to the virus and not where such exposure may have taken place. To ensure transparency of the app, the APK file of TraceTogether is made publicly available.

TraceTogether serves as a form of decentralised contact-logging and contact tracing. Due to certain confusion among the public concerning the operation of the app, its scope and its utility, the government recently announced that by the end of June it would be making available a wearable 'toggle' device for tracing purposes. While neither the toggle not Trace Together is compulsory other than for migrant workers as noted above, people are strongly encouraged to subscribe to one or other option. In recent days the Government has issued warnings to subscribers that counterfeit applications have come to its attention and therefore care needs to be taken in ensuring the authenticity of the download source.

The Smart Nation administration is working on currently making TraceTogether more inclusive or even to replace it. According to the Smart Nation and Digital Government Group "Because TraceTogether does not work equally well across all smartphones, we have decided therefore, at this point in time, not to mandate a compulsory use of TraceTogether."

2-3 Safe Entry QR Codes.

Since April, the Singapore Government has been progressively rolling out its safe entry system. Prior to the QR code option, this process was manual in that persons wishing to enter vulnerable settings such as hospitals and public buildings were required to undergo a temperature check and to have their national identity card (NRIC) details and time of entry and general health condition manually recorded.

Over recent weeks the Government has issued QR codes, initially to markets, supermarkets and food outlets. This procedure is gradually being extended to all places of commerce, business and administration which remain open for public access. Any person wishing access to such premises is required to download a QR code reader onto their smartphone. If they do not possess such technology, then the manual recording of their temperature and personal details remains an option.

On approaching the premises concerned people are required to scan the code and from there they will be transferred to another webpage which is a centralised data recording facility. On first use the individual must enter their NRIC number, their phone number and address, which can then be saved onto the application for future activation. At this stage they are instructed to 'check in' and this compliance should be monitored by the employee of the premises who is taking temperatures and allowing admission. In most situations the phone application requires a similar 'check out' practice on leaving the premises. The QR code procedure is now also required when using the mass rapid transit rail system.

Data accumulated through the QR code safe entry application is stored centrally by the Government. A website entry ensures that data, which is obviously identified, will be decommissioned after the expiration of any potential incubation period, that being 14 days.

3. Contact Tracing Justifications

Crucial in understanding Singapore's reliance on smartphone applications in its COVID control strategy is to identify the purpose for the surveillance, what type of information is needed through these surveillance and tracing technologies. Whether these purposes are achievable via technology is the central criteria for evaluation and then to consider if such purposes are in fact are exceeded. For instance, using the Bluetooth LE proximity tool is currently popular in tracing and tracking. This approach may be adequate for the initial "identification" step of contact tracing, but other known location data still might be needed to enforce quarantines or identify hotspots.

Recently Singapore has utilised AI extensively to develop faster testing capabilities, to advance vaccine research, to better perfect armband tracking devices and applying 'deeptech' to mass CT scanning diagnostics[19].

To reiterate, the main goal of contact tracing is to identify close contacts of confirmed cases. As for its extant purpose, tracing follows individual movement and plots/records human contact so that potential transmission will be revealed. It is not difficult to imagine how such data on movement and association may also present a variety of other control and social engineering purposes. In this regard identification of data subjects is crucial, as are their patterns of movement and association. Even if the data subjects are given case names (such as in Singapore) linking back to actual identity is easy and intended. Closely related is the follow-up process: informing close contacts, asking these people to stay home, and/or sharing the locations that positive cases have visited. Contact tracing is part of the larger project of using ICTs to address disease outbreaks. Again, the identities of associates will be known and shared, as will be patterns

[19] Olivia Poh, Covid-19 putting Singapore on global deeptech radar (14 April 2020), https://www.edb.gov.sg/en/news-and-events/insights/innovation/covid-19-putting-singapore-on-global-deeptech-radar.html

of movement.

The 'first generation' of contact tracing programs aim to identify close contacts after someone tests positive. These programs are usually targeted. Confirmed cases are often interviewed, and their verbal recall is supplemented by CCTV footage, card usage, and/or phone location data. Implementing these programs requires significant human intervention and rely on some pre-existing surveillance capabilities.

Pre-emptive tracing programs apply to the public at large, not just confirmed cases. Public health authorities encourage individuals to log of encounters which can quickly be referred to if a person tests positive. Follow-up actions (e.g. isolating close contacts) are facilitated, reducing the likelihood that carriers travel widely and spread the virus. As mentioned already, one low-tech method to accomplish pre-emptive contact tracing is to make people scan QR codes to register every time they enter venues. The ramifications of this data production and sharing in terms of rights of privacy, freedoms of movement and association, and containment of individual liberties are obvious.

Proximity tracking is less common in the current crisis armoury. Encounters are recorded, but the location of these encounters may be unknown. Proximity tracking is usually enabled by Bluetooth low energy. Many privacy advocates say that Bluetooth proximity tracking is the least intrusive form of contact tracing, and it is emerging as the most popular approach more likely because of its utility and low cost. TraceTogether and the Pan-European Privacy-Preserving Proximity Tracing are prominent apps in this category.

In the current pandemic, much effort and attention are aimed at diagnostic efforts. In particular, governments are using ICTs to (1) identify close contacts of confirmed cases and (2) maintain quarantines. In both these objectives participant identities are necessarily recorded, even if only to connect quarantine provisions with parties against whom they are directed. Phone-based tracking can further be decomposed into location and proximity tracing. Location tracing uses GPS and/or network information to identify the geographic location of the user. On April 10, Google and Apple announced that they are partnering to make it easier for countries to develop Bluetooth contact tracing apps.

While the general community in Singapore has been largely compliant with government tracing initiatives the adoption of TraceTogether has not been as high as necessary for effective coverage and social media contains criticisms of potentials for identified data sharing. Singaporeans traditionally are particularly concerned about the privacy of their personal health data.

Since April, in the rush of excitement about Bluetooth proximity tracing, experts are beginning to warn that "automated contact tracing is not a panacea". An automated contact tracing system is likely better than no system at all, but, where possible, such a system should augment rather than replace human contact tracers. First, human contact tracers are needed to make judgement calls about environment factors like ventilation. Second, following up with suspected close contacts involves difficult and anxiety-laden conversations, and it is the role of a contact tracer to explain how a close contact might have been exposed and provide assurance and guidance on next steps.

Quarantines may require tracing devices to sharpen enforcement. Governments initially sought to quarantine and monitor specific people, for example close contacts of confirmed cases. As the pandemic has become more serious, governments have imposed widespread "lockdown" measures, thus the quarantine maintenance programs which accompany these measures have become more widespread. While proximity tracing may be sufficient for identifying close contacts location information is needed for quarantine maintenance.

Quarantining and tracing have some interconnections insofar as they are both concerned with mapping and controlling patterns of movement. We note that it is hard to verify at what level of abstraction a given government is analysing location data, and governments are likely combining different approaches with problematic consequences for data integrity.

The recent surge in proximity apps, and many still in development, means the critical discussion remains fairly nascent particularly in Asian jurisdictions where these applications were mandated without much debate or consultation. The data integrity challenges relating to Bluetooth proximity tracing apps will become clearer as various projects are rolled out in the coming weeks and months. These are some speculative challenges:

- Bluetooth mainly addresses issues related to identification rather than follow-up. Can such limited technology address how to monitor people who have been told to stay home?
- Location can be inferred from proximity to known locations. As a result, the remit of proximity-based apps could be expanded. In the UK, the NHS has internally discussed whether the app can be retooled to enforce social distancing, for example by warning people if they spend too much time outside.
- Garnering high enough levels of adoption—50-75% of the population seems necessary. As of 4 April, about 16% of people in Singapore had downloaded TraceTogether.

- Failures in coordination between different projects could divide up the tracked population into even smaller chunks and less representative.
- Problematic data security of Bluetooth technology.

One key question about the application of technology to the control of human movement relates to the essential nature of information needed and for what purposes. Proximity may be good enough for the identification step of contact tracing, but location data will be necessary to enforce quarantines or identify clusters.

4.Singapore's Second Wave

Of the just under 50,000 COVID-19infections currently registered in Singapore, more than 90% represent migrant workers resident in hostels. This infected population started to surface in large numbers late in March. Prior to that time Singapore had relatively low local infection rates, was well managing imported infections and was regarded world-wide as a paragon of pandemic response control.

What went wrong?

The early indication of a possible outbreak was when on several occasions cases of infection were traced back to a major supermarket and shopping complex preferred by many migrant workers. When the first hostel showed a quickly spreading number of infections the Government moved to impose quarantines. However, Government inspectors and health care workers who visited this and other hostels in the early days were dismayed at the living conditions in terms of space and hygiene. It was as if migrant workers had been living under high risk conditions and little had been done to expose these to detailed scrutiny and regulation outside the exigencies of the pandemic. For instance, some hostels were determining occupancy on the assumption that a proportion of workers would be involved in shift work and therefore more men could be crammed into less space because of this rotational reality. Lock down conditions meant that these living units became unsustainable.

Once social distancing had failed and the possibility of mass relocation to less crowded conditions had passed, the authorities imposed total quarantine and with it came incubation rates of infection. The reality behind this policy was the hope that because most of these men were young and fit, the consequences of infection would be reduced. Against that was a motivation to prevent spread into the general population.

Looked at objectively, while the justifications are realist, the consequences of the control policy could be viewed as inequitable. There are two important regulatory issues on which to reflect in terms of Singapore's 'second wave' and the response to this outbreak.

1. Risk assessment - Insufficient recognition was given to a vulnerable demographic in early risk assessments party due to the social anonymity of the population. If appropriate regard had been payed to the nature of living conditions in the hostels prior to the first mass infections, then strategies could have been implemented to limit the spread before quarantine/ incubation was necessary.

2. Risk minimisation - As with other risk populations (such as the elderly in institutional care) the location and lived circumstances of this group (structurally discriminatory as they may appear) should have indicated the failure of a key control strategy such as social distancing. The timing of interventions is also important. Because mass testing of migrant workers did not occur until after major infections then this strategy did little beyond update the daily growth of the problem.

The challenge posed for the Singapore health services by the mass infections of isolated migrant workers is not dissimilar to the challenge posed by quarantined cruise ship populations, where adequate risk evaluation did not commence even before signs of an outbreak. Obviously, in any effective risk assessment, structural givens such as the nature of social and economic discrimination, and the selective application of health care are important contextual backdrops, even if they may not feature in specific control outcomes. The lessons to be learned from Singapore's experience with the infection of migrant workers emphasise the importance of early identifications of risk/vulnerability as a consequence of natural or structural discriminators as re-imagined through the pandemic. For the migrant worker sector of the Singapore population, so vital for Singapore's post-COVID recovery, having them housed in poor quality and close confined conditions was a prime risk indicator, one which diminished the availability and impact of essential manual control approaches such as social distancing and mass testing. In addition, the 'social anonymity' of their existence and the reality that their disempowered lifestyles makes them exposed to infection 'hot-spots' (such as less sanitary food outlets) further increasing their risk/vulnerability to the virus.

Another important dimension for examining social and economic discrimination as a key element in pandemic risk evaluation is that control responses can be discriminatory (or because of limited options might be precluded from avoiding discrimination). On its own admission the Government in Singapore did not move quickly enough to depopulate the hostels before the virus took hold. As a result, social distancing was not an option and it was replaced by quarantining, incubation and hopes on herd immunity. As with the failure to contain the virus within contexts of institutional aged care UK, or in prisons in the US, or for whole cities in China, internal and external factors mean that quarantine and incubation are the primary interventions, the consequences in the short term being higher infection and mortality rates and lower prospects for recovery. Add to this globally the differential death rates based on ethnicity, and the selective triage decisions based on life expectancy and control responses are proven to demonstrate discriminatory outcomes.

While control strategies may be discriminatory if the risk of discrimination was modelled along with the risk of infection then governments (and associated civil society organs or employers or service providers) might be better placed to adopt proactive or ameliorating policies for such differential impacts and in so doing pre-empt the risk of pandemic spread and control confinement.

5. Future Considerations for AI-assisted Pandemic Control

There is not space here to discuss in detail the operational and ethical challenges posed by the use of surveillance technologies and the mass data they produce as part of COVID-19 control strategies. These are presented more fully in the papers footnoted earlier, as are arguments why ethical guidelines as a regulatory frame may not be sufficient on its own to ensure that rights and liberties are protected in the transit out of pandemic controls.

In looking at the successes and failures of the recent Singapore experience, this paper suggests that AI-assisted technologies can have a positive role to play in mapping the progress of the virus both in terms of medical diagnostics and tracing/tracking regimes. But as is often the case, any unregulated roll out of AI to meet contemporary crises will carry with it concerns for the protection of personal data and civil liberties.

Where algorithmic modelling assisted with machine learning has a vital if currently under utilised or delayed function is in risk analytics. As the situation with Singapore's 'second wave' starkly reveals there are two major directions for risk prediction in which modelling would be of great benefit

- For identifying risk groups as a consequence of pre-existing structural discrimination in society, and from there specifying the nature of their vulnerability and how this can be factored into preventive control strategies; and
- Predicting the discriminatory impact of various control choices when directed against these vulnerable groups, and therefrom generating policy

to ameliorate negative control consequences or limiting control options.

Finally, one of the simplest and most effective control strategies in Singapore is preventive admonition — the daily text messages from the health authorities encouraging us to be careful, mindful and vigilant. Not much complex tech involved but that regular reminding about civic responsibility takes responsibility away from AI to protect us and brings it right back to the citizen and their inclusion.

Mark Findlay

Email: markfindlay@smu.edu.sg

Bio:The Director of the Centre for AI and Data Governance, Law School, Singapore Management University.The Centre researches ethical AI applications in Singapore, personal data protection, privacy, and a range of community, industry and commercial concerns about AI and mass data sharing

JAPAN

Challenges of AI and Data Utilization and Governance in Japan Emerging from the COVID-19 response

Arisa Ema

1. Japan's Policy on COVID-19 and AI/Data[20]

The crisis of viral pneumonia of unknown origin began in Japan at the end of 2019. The World Health Organization (WHO) confirmed the detection of the new coronavirus on 14 January 2020. Japan confirmed its first COVID-19 case on 16 January 2020, involving a man who had returned from Wuhan, China. On 28 January, the first domestic transmission of COVID-19 involving three people, including a Japanese bus driver with two tour passengers from Wuhan, was confirmed in Japan. On the same day, the government passed a cabinet order classifying COVID-19 as a "designated infectious disease" under the Infectious Disease Law and a "quarantinable infectious disease" under the Quarantine Law, which facilitated the enforcement of compulsory hospitalization, restrictions on commerce, and inspections of people entering the country. At the end of January, many Japanese citizens returned from Wuhan by chartered flights. On 30 January, the government established the novel coronavirus response headquarters.

The passengers on the Diamond Princess cruise ship that returned to the Yokohama Port on 3 February were infected with COVID-19. Consequently, the government did not allow over 3,700 crew members to disembark and placed them under 14 days of quarantine. Additionally, the first death in Japan was confirmed on 13 February, and the number of infected people exceeded 100 on the 21 February. On 13 March, the Act on Special Measures for Pandemic Influenza and New Infectious Disease Preparedness and Response was partially amended. A state of emergency was declared in seven prefectures on 7 April and throughout the country on 16 April. The declaration requested self-restraint in going out, closing schools, and holding events; lockdown or isolation was not enforced. Compulsory measures taken in other countries are based on legal grounds that the right to freedom of trade and movement may be limited under certain conditions. Japan's current laws, on the other hand, have no such basis. Therefore, measures were based on requests rather than enforceable legal revisions.

[20] This article was released as a result of fruitful discussions and supports from the following individuals. Hideaki Shiroyama and George Shishido (The University of Tokyo), Fumiko Kudo (Osaka University), Takanori Fujita (Centre for the Fourth Industrial Revolution Japan), Hiroshi Nakagawa (RIKEN AIP Center).

People follow requests, even when it is not compulsory, possibly because Japan is under strong peer pressure of "how people see it." There are no legal penalties for not exercising self-restraint. However, for example, news about the shops and stores that did not voluntarily close could lead to social sanctions. On the other hand, social sanctions have gone too far. Based on the news, infected people and the organizations they belonged to are identified and often criticized in the real and virtual worlds. It has also led to discrimination and bashing not only of the parties involved but also of related organizations and communities. Consequently, in the early stages of infection, infected people and the organizations to which they belonged apologized for causing anxiety and inconvenience to many people, including those in the community. From this perspective, a clear insight that voluntary restraint can not only help prevent infection but also avoid bothering others can be observed among people.

Subsequently, the "Stay Home Week" commenced from 25 April to 6 May. The state of emergency was lifted for 39 prefectures on 14 May and for all prefectures on 25 May. Alerts were issued in June in some areas, including Tokyo, but were lifted on 11 June. However, the number of cases has continued to increase nationwide since July. Nevertheless, the number of seriously ill patients has not increased yet; therefore, a state of emergency has not been declared again. The government launched a "Go To Campaign" on 24 July to encourage tourism, which has disrupted the balance between economic activity and public safety.

With the nationwide curfew and closure of schools, telework and distance education have been introduced together with the remote and online diagnosis for the first time, which had not been advanced in Japan before. This has promoted digitalization in Japan. On the other hand, it also revealed that even data sharing before artificial intelligence (AI) use was difficult. This article summarizes the current state of COVID-19 and the use of AI and data in Japan and introduces issues that have become evident.

2. Data and AI utilization to compete with COVID-19.

2-1 AI Research and Supercomputers

The Artificial Intelligence Japan Research and Development Network (AI Japan), which promotes information transmission and cooperation on the research and development of AI, released information about the "AI-enabled research activities for COVID-19" in May 2020. The overview of the survey conducted among members of universities and public institutions is as follows: (1) infectious disease control by AI: genome analysis, diagnosis prediction/support, testing support, and emergency support; (2) transmission suppression of the infectious disease by understanding human social behavior through AI: infection simulation, social behavior analysis; (3) detection and treatment of infection by AI; (4) AI usage for remote circumstance enhancement: education, medical care, nursing care, telework, robots, etc.

Regarding data utilization and AI, supercomputers are also important for simulation and computation. RIKEN's supercomputer "Fugaku (富岳)" won the first place in four categories in the world's supercomputer ranking announced in June 2020. Currently, research is being conducted to identify therapeutic drug candidates for COVID-19 and simulate the prediction of viral droplet infection and countermeasures using the general-purpose supercomputer "Fugaku (富岳)" with low power consumption and high performance. It is important to promote research and development of AI technologies for analysis, including data that can be used as the basis for such technologies, and hardware such as supercomputers.

2-2 Contact Confirming Application: COCOA

Understanding an infected person's behavior and the information about people in close contact with the infected person can help prevent a pandemic. In this context, contact tracking and tracing applications have been introduced in many countries. In Japan, the "Anti-COVID-19 Tech Team" was launched in April, and discussions on applications were held. The Code for Japan, a general incorporated association, had already developed a Bluetooth contact confirming app, and other private companies, including Rakuten Inc., had expressed interest in developing apps. Therefore, several apps were developed simultaneously. However, on 4 May, Google and Apple Inc. announced that the contact-tracing tool will be restricted to one public health app per country and must be built by public health authorities. This eventually led the Ministry of Health, Labour, and Welfare to run an app called COVID-19 Contact Confirming Application, COCOA.

The app uses Bluetooth to match a person who has tested positive for COVID-19 with a person who has been in close contact with the infected person for more than 15 minutes within one meter, using a smartphone or other device. It does not perform contact tracing like the Singapore government app; therefore, the term contact confirming is used in Japan. It does not record any personally identifiable information, such as the location of the contact or the individual's phone number, and contact information is automatically deleted after 14 days. One can also withdraw consent at any time and delete the app. The PCR-positive person receives a processing number from the Health Center Real-time information-sharing System on COVID-19 (HER-SYS) and registers himself/herself in the app. In principle, health authorities do not obtain personal information from the COCOA. If a person has been confirmed to have had contact with an infected person, the contact information of the nearest Returnee and Contact Consultation Center will be displayed to the contacted person. If the contacted person has symptoms, he/she will be informed of the visit. On the other hand, those who do not have symptoms and whose relatives are not suspected of being infected will not be eligible for medical checkups or tests[21].

Regarding this contact confirming application, the Research Center on Ethical, Legal, and Social Issues of Osaka University published 10 perspectives to help users decide whether to download the app and conducted a somewhat real-time technology assessment. Version 0.9, which was published on 12 May, suggested the following three points for app developers and providers to increase the amount of information for users to make informed decisions: (1) specify the app's purpose, such as whether it is a means for experts to identify close contacts, a means to promote behavior modification of individuals who are notified or both; (2) conduct a system-wide privacy impact assessment should be performed instead of only assessing the app because collaboration with the HER-SYS is scheduled; (3) Enlightenment activities on the meaning and accuracy of close contact, alternatives for people who do not have smartphones and cannot use apps, and consideration of safeguards against discrimination and prejudice against COVID-19 positive people, contact people, and those who live or engage in economic activities in contact areas[22]. The "Privacy and security evaluation and considerations for system operation of 'Contact confirming application and related system specification'" released on 26 May by the "Expert Panel on Contact Confirming Applications[23]" organized within the Anti-COVID-19 Tech Team, includes points to remember, such as ensuring transparency in the design and operation of apps, inclusion of app users to lessen unfair discrimination, and limitations on the purpose of use. On the other hand, a system-wide privacy impact assessment, including the HER-SYS, has not been published as of 22 July.

The app was released on 19 June but was shortly hit by a bug on its launch date, along with several problems, including a positive registration bug. The issue was resolved in the subsequent update, and as of 22 July, about 7.97 million downloads have occurred, representing about 6% of the population. The number of positive registrations was 381.

2-3 The Ministry of Health, Labour, and Welfare and the LINE survey

Downloads are a challenge for new apps. On the other hand, many Japanese have already downloaded a communication app 'LINE' to their smartphones and other devices. As of December 2019, LINE had about 83 million active users in Japan (population coverage rate of 65.8%), 86% of whom were daily users.

The Ministry of Health, Labour, and Welfare signed an "Agreement on the Provision of Information Contributing to COVID-19 Cluster Countermeasures"

[21] Ministry of Health, Labour, and Welfare, About COVID-19 Contact Confirming Application, https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/cocoa_00138.html

[22] Atsuo Kishimoto, Fumiko Kudo, 10 perspectives on COVID-19 Contact-Confirming Application (COCOA) and ELSI, https://elsi.osaka-u.ac.jp/research/443 (in Japanese)

[23] "Privacy and security evaluation and considerations for system operation of 'Contact confirming application and related system specification' " Expert Panel on Contact Confirming Apps, https://cio.go.jp/sites/default/files/uploads/documents/techteam_20200526_02.pdf

with the LINE Corporation on 30 March 2020, and conducted a "National survey for COVID-19 countermeasures" in four installments commencing from the end of March to the beginning of May 2020[24]. Under the agreement, data will be anonymized so that it does not contain personally identifiable information and cannot be used for purposes other than originally intended. Additionally, data are deleted after a certain period. The survey was conducted by LINE Corporation and will be analyzed by the Ministry of Health, Labour, and Welfare. The average number of respondents to the survey was approximately 22 million (about 26% of active users). This number is close to 20% of Japan's population.

Professor Hiroaki Miyata of Keio University, who was involved in the analysis of this large-scale survey with the Ministry of Health, Labour, and Welfare, explained that it was necessary to grasp the actual situation to supplement the parts that could not be obtained by the PCR test. Many PCR and antibody tests need to be performed to grasp the actual condition of COVID-19 cases. However, in April, Japan was not equipped with the system compared with other countries. Therefore, one purpose of the survey was to forecast medical demand based on data other than PCR testing. Additionally, the survey showed that there were differences in the results according to the occupational groups of patients with fever.

2-4 Use of private sector data

As in the aforementioned LINE survey, the government has employed a new method of gathering information using a private company's platform. In the LINE survey, the data reportedly does not match with any other source or platform. On the other hand, the movement of B2G (Business to Government), wherein the government utilizes the user data usually acquired by private enterprises, was also promoted in response to COVID-19. Specifically, the Cabinet Secretariat (IT General Strategy Office and Novel Coronavirus Response Promotion Office), the Ministry of Internal Affairs and Communications, the Ministry of Health, Labour, and Welfare, and the Ministry of Economy, Trade, and Industry requested platform service providers (IT and Internet giants) and mobile communications providers to provide statistical data that will contribute to preventing the COVID-19 spread. In this case, anonymized data that does not identify individuals are utilized[25].

The website of the Cabinet Secretariat's "COVID-19 Information and Resources" now shows the transition of human flow in Tokyo and other urban areas. Data can be obtained by mobile phone service providers to obtain gender, age, and other information from the number of mobile phones located in each base station area and the contact information, or by obtaining GPS information from an agreed user through an affiliated location app. The use of such statistical data is expected to help verify the effectiveness of measures to ensure social distance,

[24] Ministry of Health, Labour, and Welfare, Information about what we have learned from the "National survey for COVID-19 countermeasures," https://www.mhlw.go.jp/stf/newpage_11244.html (in Japanese).

[25] In response to this request, Yahoo Japan Corporation has incorporated transparency in its agreement with the advice of experts.

such as requests to refrain from going out, verify the effectiveness of measures implemented as cluster measures, and improve the accuracy of cluster measures to be implemented in the future.

3.Challenges highlighted through COVID-19

3-1 Pre-AI Issues

The Government of Japan has been promoting its digital transformation policy under the concept of the Society 5.0, a human-centered society that simultaneously achieves economic development and resolution of social issues, through a system that integrates cyberspace and physical space. However, COVID-19 revealed that Japan was not ready to move into Society 5.0. Particularly, the data distribution problem, which has been emphasized for a long time, became clear. On the one hand, as mentioned above, the fact that government and private companies signed an agreement on COVID-19 to promote the use of data can be regarded as a step forward. On the other hand, regarding the provision of data from the government to the private sector, there is an example of information-sharing through an open-source, in which the Tokyo Metropolitan Government disclosed the number of people who tested positive in Tokyo, their attributes, and the number of call center consultations.

On the other hand, the government was unable to provide a special flat-sum payment of 100,000 yen to each Japanese resident because the My Number card, which could be used as existing infrastructure, would cause confusion in some areas. Information-sharing between the central and local governments and the medical institutions was also found to be ineffective. In some areas, including Tokyo, the number of cases is counted in analog form, and it takes three days for a person to be announced as infected. In May, 111 people were not included in the statistics because the Tokyo Metropolitan Government reported the number of infections by fax. Furthermore, it is difficult to conduct unified discussions regarding medical data because the private and government sectors have different guidelines for the protection of personal information.

To solve these problems, the government started operation of the Health Center Real-time information-sharing System on COVID-19 (HER-SYS) in May. Under this system, the national government, local governments, and medical institutions will be able to centrally manage the names, genders, contacts, test results, and admission/discharge status of examinees for PCR (genetic testing) and antigen tests for COVID-19, and share information on those infected. However, as of 14 July, one quarter or 39 local governments were unable to use the system, including Tokyo. Therefore, there is no nationwide information aggregation system in Japan as of 22 July.

3-2 Challenges from an AI and data governance perspective

The discussion of contact apps presents not only the tradeoff between public health and privacy but also the challenge of creating and explaining user benefits in data distribution. In AI and data governance, it is necessary to promote data distribution and sharing; however, there is a problem that direct user benefits are not seen.

This problem is not limited to COVID-19 and has been emphasized for a long time. Particularly, there are many B2B (business to business) companies in Japan, not B2C (business to consumer) companies. In other words, there are many cases where company A, which provides AI and data services, provides the system to company B, which is another vendor, and company B provides the actual services to the users. In this case, company A does not have direct access to AI and data service users or consumers. Furthermore, if company A provides users' personal information to the government or other private companies for purposes other than originally intended, such as for public safety, it is necessary to obtain consent again. Since it is difficult to see the direct return of benefits to users and consumers, it becomes necessary to consider how to explain the need for obtaining the users' consent again, how to develop a business model, how to design incentives for users and consumers, and where to look for problems in the event of an incident. When explaining the potential benefits and disadvantages to consumers and users, there is a possibility of a long supply chain, since the companies that explain the benefits and disadvantages differ from those that provide the data and AI technology.

The length of the supply chain complicates not only the difficulty of explaining AI technology and data usage to users but also the issue of responsibility for accidents and incidents. Company B, which is in direct contact with company A, explains AI services to users and consumers; however, this does not mean that company A does not have to consider ways to inform users. Furthermore, it is inappropriate for company B to distort company A's explanation to inform users and consumers. When an accident or incident occurs, how far back in the supply chain should the responsibility be taken? This requires a framework that enables system developers, service providers, business users, data providers, consumers, users, and other stakeholders to review management and governance practices[26].

3-3 What Does the Privacy and Human Rights Debate Mean?

In Japan, examples of new ways of living in response to COVID-19 include maintaining social distance, washing hands while wearing a mask, refraining from moving to infection-prevalent areas, and using contact confirming applications. However, as mentioned before, people's activities during emergencies cannot be legally restricted in Japan. Therefore, each person is requested to practice the

[26] In June 2020, the authors released a policy proposal entitled "RCModel, a Risk Chain Model for Risk Reduction in AI Services." The model classifies risk factors for providing AI services into three layers: (1) technical factors, (2) code of conduct factors for service providers, and (3) user understanding, behavior, and usage environment factors. https://ifi.u-tokyo.ac.jp/en/news/4815/

basic infection countermeasures. Experts have raised questions about the extent to which contact confirming apps will be used on a request basis, and whether it will be meaningless at this population coverage. On the other hand, it is necessary to discuss why the use of such information is not progressing, considering the ideal form of AI and data governance and public values and awareness.

An international poll on COVID-19 by the Gallup International Association for 30 countries in March 2020 asked about the people's willingness to sacrifice some human rights if it helped to prevent the spread of the infection. An average of 75% of people agreed among 30 countries, while only 32% agreed in Japan, the lowest among 30 countries. There was a gap with Austria (95%), which ranked first, and the United States (45%), which ranked 29th. In the second survey of 18 countries conducted in early April, an average of 81% of people agreed in 18 countries, while 40% agreed in Japan, remaining at the bottom again. On the other hand, it is also true that the infected people in the early days in Japan were identified and slandered in various ways on SNS and in real life, and the families of the infected people or people of the same organization and community were forced to leave school or lose their jobs. What does "human rights" mean to the Japanese? We also need to consider ways and measures to prevent injustice and discrimination.

4.The Future of AI and Data Governance in Japan

International discussions on AI and data governance began in 2016. Various guidelines and policies were released from each country, industry, academia, civil society, and international organizations, and the OECD Policy Observer website provides a comprehensive view of themes and countries[27]. Japan had begun discussing the challenges posed by AI technology at a relatively early stage since 2016. The Cabinet Office released the "human-centered AI societal principles" in March 2019, and the Conference toward AI Network Society of the Ministry of Internal Affairs and Communications released the "AI Utilization Guidelines" in August 2019, and has been examining matters that AI service providers, business users, and consumers should consider.

Therefore, 2019 can be considered as a milestone year for the international consideration of AI governance. Discussions are held on an international and interdisciplinary basis, and several reports have been released that compile various guidelines. Table 1 compares key words in reports prepared by the Chinese Academy of Sciences (2018) and Harvard University's Berkman Klein Center (2019). The table shows that the essential values are generally the same for both. Besides the traditional information technology values such as security, safety, and privacy, AI governance discussions have three additional characteristics: Fairness,

[27] OECD, OECD AI Policy Observatory, https://oecd.ai/

Accountability, and Transparency, called FAT in short. It is also called FATE with Explainability. However, there is a case in which the output result of AI becomes unfair and discriminatory through the learning data bias, algorithm bias, and (unconscious) influence of the designer due to the discrimination and prejudice that exist in the society.

Table 1 Reports by researchers at the Chinese Academy of Sciences (https://arxiv.org/abs/1812.04814) and the Harvard University's Berkman Klein Center (http://wilkins.law.harvard.edu/misc/PrincipledAI_FinalGraphic.jpg))

Chinese Academy of Sciences (2018)	Harvard University's Berkman Klein Center (2019)
Humanity	International Human Rights
Collaboration	Promotion of Human Values
Share	Professional Responsibility
Fairness	Human Control of Technology
Transparency	Fairness and Non-discrimination
Privacy	Transparency and Explainability
Security	Safety and Security
Safety	Accountability
Accountability	Privacy
AGI	—

The discussion on AI is about value, and COVID-19 has forcefully highlighted some of its aspects. In the face of the COVID-19 pandemic, many people in many countries believe that some restrictions on individual rights are inevitable for the public good. However, the question is about how long this emergency will last. Will it end when the vaccine is developed, when herd immunity is confirmed, or when the number of infections and deaths have flattened and settled? In the current situation where the possible onset of the second or third wave is unknown, it is desirable to collect data during this fallow period. Ideally, the data should always be available rather than for a limited time. In medical and health care areas, daily data and in-hospital data may be important factors in making decisions. Detailed personal information is needed to provide personalized and accurate treatment and medical care. Furthermore, when considering public safety measures, AI can be used to collect data on who is in contact with whom, what kind of situation changes have occurred, and establish preventive measures against the spread of infection through data analysis. The goal is to establish a framework for the distribution of data utilization that protects privacy and security and ensures fairness, transparency, and accountability[28].

On the other hand, both during and before COVID-19, it is essential to scrutinize the transparency of whether the acquired data will be used for other purposes and whether there is corporate accountability. That the collection and accumulation

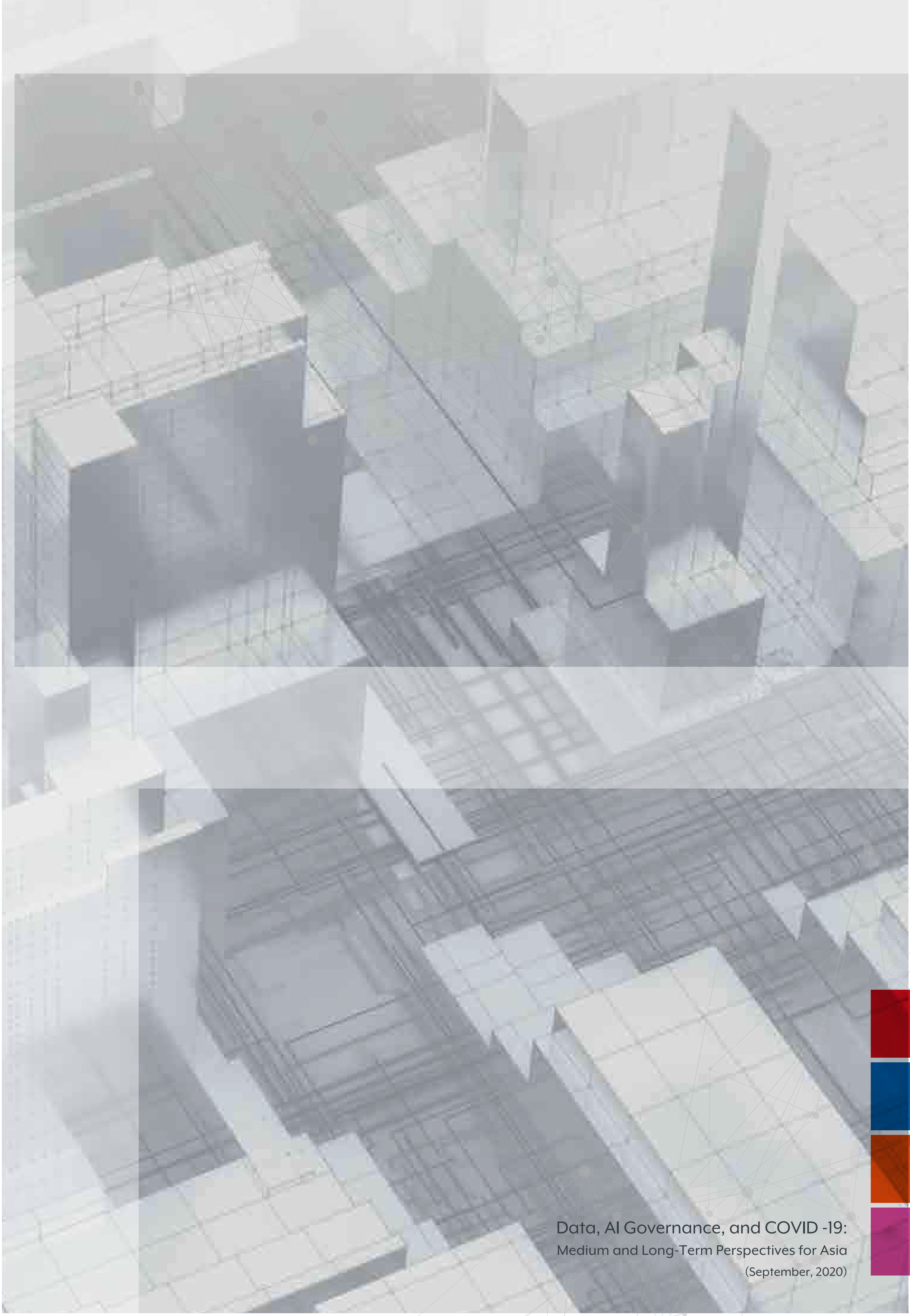
[28] The World Economic Forum Centre for the Fourth Industrial Revolution, Japan has proposed the framework of "Authorized Public Purpose Access (APPA)" on the coexistence of data utilization and personal information protection with the health care domain. This allows data to be used for public purposes without consent if a social consensus has been reached while giving due consideration to human rights such as privacy and the companies that hold the data.

of data and the analysis and prediction of AI technologies could undermine equity and foster discrimination has become a challenge in many countries. In an emergency, what decisions and actions do we take, and what values do we value and act? The "human-centered AI societal principles" published by the Cabinet Office also emphasize human dignity, diversity and inclusion, and sustainability as central values in the issues surrounding AI ethics and governance. Beyond the superficial issues of future data handling, COVID-19 raises fundamental questions about AI ethics and governance.

Arisa Ema

Email: ema@ifi.u-tokyo.ac.jp

Bio: Project Assistant Professor, Institute for Future Initiatives, University of Tokyo and Visiting Researcher at RIKEN Center for Advanced Intelligence Project in Japan.



Data, AI Governance, and COVID -19:

Medium and Long-Term Perspectives for Asia

(September, 2020)