Surveillance & Society

Opinion

The Far-reaching Implications of China's AI-powered Surveillance State Post-COVID

Elise Racine

University of Oxford, UK
elise.racine@ndph.ox.ac.uk

Abstract

The COVID-19 pandemic has vastly accelerated the digitalization of public health practices worldwide. In doing so, it has fostered a new class of pandemic-related technological solutions, a subset of which utilize artificial intelligence for contact tracing purposes. The People's Republic of China has not been immune from this rush to implement these novel tools. But there is a darker element to the country's Alipay Health Code mobile application that extends beyond pandemic preparedness. With ambitions to further incorporate the app into their already vast surveillance apparatus, China is on the precipice of setting a dangerous precedent for pervasive, state-sponsored automated social control. In such a world, we may see health tools co-opted into systems that score individuals on their political fealty. As such, they have the potential to severely undercut democratic ideals by restricting the freedom to dissent necessary to uphold such values. They would do all this under the guise of promoting collective wellbeing.

Introduction

Considering China's foreign involvement in the Majority World—including via the Belt and Road Initiative—these developments have major global implications. Various regimes have already started to emulate China's model of digital authoritarianism, facilitated by these political-economic arrangements. As this model continues to be exported abroad, it could gain additional footholds in fragile and susceptible states. By suspending normal politics, the COVID-19 crisis may further facilitate this expansion. To further explore this prospect and the associated consequences, I draw from biopolitics and the recent shift towards health securitization. As part of this (brief) discussion, I examine how these AI-powered public health tools not only extend the surveillant dimensions of the systems in which they are imbedded, but can significantly reproduce and/or augment inequities. The possible impact, particularly for the already vulnerable, means one thing: we must pay attention to what is happening in China.

Visions of artificial intelligence (AI) surveilling humankind have captured our collective consciousness. From *The Matrix* to *Westworld* to *Star Trek*, these narratives have devised a variety of technological futures ranging from despotic to utopian. In doing so, they have provided fodder for journalists, politicians, and academics alike. The figures dominating these stories have been both real and imagined, including tech giants like Amazon and Google. As the world's leading seller of AI-powered surveillance equipment with a reputation for extensive—at times dystopian—state surveillance, the People's Republic of China has garnered its fair share of attention. But something we are only beginning to grapple with is how these surveillance capabilities have changed and expanded with the COVID-19 pandemic and the global implications of such developments, especially in view of China's foreign involvement in the Majority World. My focus stems not only from my opinion that the subject matter is one of great import, but my observations that current discourses have fallen short. In engaging in the following discussion, I hope this

Racine, Elise. 2023. The Far-reaching Implications of China's AI-powered Surveillance State Post-COVID. *Surveillance & Society* 21 (3): 269-275.
https://ojs.library.queensu.ca/index.php/surveillance-and-society/index | ISSN: 1477-7487

piece may act as an impetus for further deliberation and, ultimately, action. Considering the National Health Commission's recent announcement that all Chinese residents will be provided with a "fully functional digital health code" (Zhao 2022), I believe it is a time-sensitive and critical endeavor.

Digital Contact Tracing: An Introduction

Evidence suggests that the likelihood of pandemics will only continue to increase, a possibility which highlights our need for more effectual surveillance technologies. By enabling the robust, efficient, and timely analysis of huge amounts of data, artificial intelligence has the potential to help decision-makers better respond to, manage, and even prevent infectious disease outbreaks (Malik et al. 2021; Wong, Zhou, and Zhang 2019). This could reduce harm, disruption, and the loss of human life. Considering the promise associated with AI-powered tools, it is perhaps unsurprising that the COVID-19 pandemic has vastly accelerated the digitalization of public health practices and fostered a new class of pandemic-related technological solutions. Around the world, various public, private, and state actors have rushed to implement these novel tools—many of which have been used for contact tracing, or the process of identifying the individuals with whom an infected person has recently had contact.

There is no doubt about it, contact tracing is an important communicable disease control measure and has been crucial to stopping the transmission of SARS-CoV-2, the virus which causes COVID-19. Historically, the process has involved interviews and manually tracking contacts—actions which are time-consuming and difficult to scale during a global pandemic. Innovative technologies, particularly mobile phones, have made it possible to digitalize these efforts. If widely adopted, digital contact tracing applications have the potential to be more effective than traditional tracking methods. The hope is that by identifying and interrupting possible infection chains earlier, these digital methods may also help ease restrictions and facilitate a quicker return to normal social life (Corona-Warn-App 2022).

Digital contact tracing can take several forms. For instance, contacts can be recorded via various technologies, specifically global positioning systems (GPS), Bluetooth, ultrasound, closed-circuit television (CCTV) with facial recognition, or GEO-QR code tagging. Most applications, however, use either GPS or Bluetooth to estimate the proximity and duration of a person's exposure to an individual with COVID-19. In some countries, these data have been supplemented with intelligence gathered from credit card transactions, security footage, and other sources (Kharpal 2020b). In China, authorities have mobilized the country's extensive surveillance apparatus and employed a mix of travel records, CCTV cameras, drones, and location data from cellphones to trace the coronavirus' spread and enforce quarantines (Kharpal 2020a). Such actions have not only introduced and amplified new data sources for the purposes of infectious disease surveillance, but demonstrated how AI capabilities can be overlayed with older generation devices to amplify the surveillant dimensions of these systems. They also raise important questions around function creep and the possibility for mass surveillance—both now and in the future.

China's Alipay Health Code Application: An Exploration

But the growing reliance on digital pandemic surveillance tools does not exist in vacuum. This becomes increasingly clear as I delve into my case. Prior to the COVID-19 pandemic, the scope of China's surveillance apparatus was already vast, employing advanced technology such as GPS tracking, artificial intelligence, and facial recognition. The country's use of big data to respond to the crisis has enabled even more comprehensive surveillance, serving as an opportunity to introduce new technologies, merge existing ones, and expand surveillance functionalities. While there are several directions this piece could take, I have elected to center my attention on the Alipay Health Code mobile application as its mechanics most closely resemble the digital contact tracing solutions utilized by numerous entities worldwide.

The Alipay Health Code app has been an integral component of China's pandemic response. First introduced in Hangzhou, the application was created by the local government with the help of Ant Financial, a sister company of the Chinese e-commerce giant Alibaba (Mozur, Zhong, and Krolik 2021).[1] This public-private partnership mimics trends seen in many other countries, including Germany, Switzerland, the United Kingdom, and others. The system has since been rolled out nationwide and is in use in 200+ cities (Mozur, Zhong, and Krolik 2021). Its intended purpose is to automatedly determine who is and is not a contagion risk. Individuals sign up through Alipay—Ant's popular mobile and online payment platform known for its broad reach. All-encompassing, it enables users to do everything from managing their finances to choosing insurance schemes to ordering in from their favorite restaurants. For the Health Code app, individuals are asked to input a variety of personal information, including their national identification (ID) number, phone number, residential address, biometric selfie, recent travel history, body temperature, and any COVID-19 symptoms. Public data are used to verify self-reported information in real-time.

The software uses these responses to generate a unique QR code (a type of matrix barcode) in one of three colors—green, yellow, or red. Those with a green code may move about unrestricted. A yellow code means the user is required to quarantine at home for seven days. Individuals with red codes are to be treated and quarantined either at home or in a centralized location for 14 days. This QR code is then scanned by authorities and, depending on the locality, required to access public spaces, transit systems, and buildings. These can include apartment complexes, offices, subways, grocery stores, restaurants, and malls. The codes can also be used to bar users from entering or exiting certain regions. Each time a person's code is scanned, their identifying code number and current location are sent to not only the system's servers, but the police—allowing the authorities to track people's movements over time (Mozur, Zhong, and Krolik 2021; Andersen 2020).

This has, understandably, incited concerns, particularly around setting a worrisome precedent for pervasive, automated social control (Andersen 2020; Mozur, Zhong, and Krolik 2021; see also Zhao 2022). Authorities, for instance, have yet to provide details into how the system classifies individuals, what data are stored where and for how long, and how this information may be used moving forward. There is also no clear means of contesting your code with some individuals reporting being unable to change erroneous "red" designations. Others worry that the app could be coopted and morphed into a more general tool that persists beyond the pandemic and enables the Communist Party of China (CCP) to incorporate these new surveillance capabilities into the broader surveillance apparatus—ultimately leading to tighter social control in the long-term.

This technological future already appears to be happening to some degree. Some extensions, on the surface, appear more bizarre than ominous. In Xining, the software has been repurposed to help boost the economy by unlocking coupons to local stores. Shanghai officials have shared their desire to transform the app into a digital assistant for accessing a variety of local services. But officials in Hangzhou are exploring how to expand the health code to rank citizens with a personal health index score based on how much they sleep, how many steps they take, how much they smoke and drink, and other unspecified metrics (Gan 2020). To this aim, authorities have started linking the app to citizens' medical records. Perhaps most troubling, however, is a recent announcement that the CPP intends to expand and centralize the system into a national, integrated health platform that supplies each resident with their own digital health code (Zhao 2022).

Delving into the International Implications: A Caution

This phenomenon of adopting a system of surveillance for one purpose and using it past these originally aims is known as function, or mission creep. For example, health tools with codes like these could also be misused to score an individual's perceived political pliancy and fidelity, and crackdown on dissenters (Andersen 2020). In fact, there are reports of authorities in the province of Henan utilizing the COVID app

[1] Chinese government officials have also collaborated with Tencent—the tech giant responsible for WeChat—to develop a similar COVID-19 tracking system using QR codes to track users' health statuses.

to restrict the movements of some residents following protests in the region (Wong and BBC Chinese 2022). Hundreds of customers who had lost access to their funds after four local banks froze deposits had planned to travel to Zhengzhou to protest, only to find their health codes had suddenly turned red despite their most recent COVID-19 test results being negative. These individuals were forced to quarantine and blocked from public transportation, etc. With their movement curtailed, the protests fizzled. The red code appears to have only targeted depositors.

Such surveillance creep has historical precedent. Capitalizing on other major events in the past (e.g., 2008 Beijing Olympics, 2010 World Expo in Shanghai), China has used these as opportunities to introduce new surveillance tools that long outlast their original purpose (Mozur, Zhong, and Krolik 2021). The global relevancy of these developments is clear when we consider China's Belt and Road Initiative—a prime and ready vehicle through which China can further disseminate their model of digital authoritarianism. Launched by Chinese President Xi Jinping in 2013, the US$1.3 trillion+ initiative is a multifaceted economic, geopolitical, and diplomatic undertaking (Kurlantzick 2020; Bhattacharya et al. 2019; Habib and Faulknor 2017). It aims to create a vast network of infrastructure projects across Europe, Asia, Africa, and the Middle East—including telecoms, roads, railways, power grids, and ports. While tooting to boost economic interconnectivity and development in the 65+ partner countries involved, the project epitomizes China's ambitions to solidify its standing as a global superpower (Habib and Faulknor 2017; Morgan Stanley 2018). But in the process of doing so, the project could massively "shift the balance of power between the individual and the state worldwide" (Andersen 2020).

There are fears of China supplying turnkey AI-powered surveillance systems to other actors—especially in places where democracy is fragile or nonexistent—creating an authoritarian bloc with the capacity for total social control (Andersen 2020). As Andersen (2020) so eloquently elucidates, "the world's autocrats are usually felled by coups or mass protests, both of which require a baseline of political organization." The freedom to unite and dissent is, in other words, a vital component of democracy. However, China's vision of the future, one dominated by automated surveillance systems, risks extending this panoptic gaze to the point where such rights are all but annihilated. Such developments would be a continuation of a decades-long campaign for total social control, the dire consequences of which have played out again and again in the Tibetan Autonomous Region, Xinjiang, and elsewhere.

These examples may become more widespread as other regimes learn from China how to manipulate mass digital surveillance systems. As it currently stands, Chinese technology companies have already helped foreign governments develop the surveillance capabilities necessary to target opposition groups (Kurlantzick 2020). These tools have been supplemented by training offered by the CCP to interested Digital Silk Road recipient countries on how to monitor the internet in real time (Kurlantzick 2020). For instance, Huawei technicians embedded within cybersecurity forces in Uganda and Zambia helped these governments spy on political opponents, including intercepting encrypted communications and using cell data to track their movements (Parkinson, Bariyo, and Chin 2019).

In Zimbabwe, China's digital projects include a partnership between the government of Emmerson Mnangagwa—autocrat Robert Mugabe's authoritarian successor—and the Gunagzhou-based company CloudWalk Technology to develop a national facial recognition program (Kurlantzick 2020). The contract requires the Zimbabwean government to share its citizen biometric data with Cloudwalk, a decision on which the Zimbabwean people were not consulted (Chutal 2018; Kurlantzick 2020). Not only could the collaboration help Mnangagwa's government, which has a poor human rights record, censor its citizens, but it provides CloudWalk with a rich dataset to fine-tune its software's abilities to identify other ethnicities—a valuable capability that could be exported to other contexts (Kurlantzick 2020; Chutal 2018; Hawkins 2018). As facial recognition systems have formerly had difficulty reading racially minoritized faces, these improvements could enable these systems to surpass those produced by American and European firms. While these examples are certainly disconcerting on their own, perhaps the most troubling aspect of the above accounts is the fact that these are just several of many. Others span Vietnam, Sri Lanka, Serbia, Ethiopia, Kenya, Mauritius, Egypt, Ecuador, and more.

But how does this all relate to the COVID-19 pandemic? Faced with a crisis of epic proportions and an urgent need to monitor their populaces in novel ways, governments worldwide have turned to digital surveillance tools to save the day. This has only fueled the demand, particularly in developing states, for Chinese AI-powered surveillance technologies (Kurlantzick 2020). In response, the CCP has linked the Digital Silk Road to the Health Silk Road, a subset of the Belt and Road Initiative that not only supports health infrastructure but offers an ideal platform for the country's further involvement in global health governance. China has recently doubled down on its efforts to recast itself as a responsible global health leader. The Health Silk Road narrative serves a political purpose in legitimizing the rule of the CCP. But as the Digital Silk Road expands, we need to be critical of China's influence on recipient states, and how these digital tools may be co-opted into mass surveillance systems used for purposes other than pandemic control.

The Biopolitics of It All: A (Brief) Discussion

The significance of these events is further impressed upon when we consider how as emerging instruments for obtaining, compiling, and categorizing information, digital infectious disease surveillance technologies are largely consistent with preceding modes of governmentality. This includes building on top of prior biopolitical technologies of calculation and categorization. In addition, these AI-powered tools extend these modes into novel spaces, adding to the surveillant dimensions of such systems. Due to the portability of mobile devices, for instance, contact tracing applications are readily accessible and easily integrated into modern life. The convenience and portability of such technologies have the potential to not only cultivate expectations of consistent surveillance but enable more opportunities for discipline—including from authorities.

As Dencik et al. (2019: 873) explain, new sources of data are fundamentally changing "the kinds of information valued and what is 'knowable' and therefore acted upon." When discussing the normalization of the body, Michel Foucault (1978) emphasizes that the more something is known and discussed, the more we become preoccupied with what is considered normal and the more intimately that thing is controlled. In sorting individuals into sensitive health-related categories these algorithmic systems can help secure the boundaries between healthy/unhealthy, us/them, or exclusion/inclusion. Such delineations have the potential to create and reinforce new and existing (a) disparities and (b) justifications for discrimination and exclusion due to such statuses (Terry 2018). The biopolitical logic inherent in these tools is especially concerning when we consider the profound shift in global health governance that has occurred over the last several decades and resulted in health issues increasingly being labelled security threats.

This transition towards health securitization has been characterized by the suspension of normal politics and an urgent call for unprecedented preventative measures. In legitimizing the use of extraordinary measures that bypass democratic procedures and other legal constraints, security politics can cause lasting institutional changes that make reactivating security rhetoric and processes easier—which can in turn accentuate inequities. This self-reinforcing tendency is dubbed the "'emergency trap' of global security" (Hanrieder and Kreuder-Sonnen 2014: 335). We may see something similar happen in the wake of the COVID-19 crisis in which it becomes easier to normalize the AI-powered surveillance systems emerging now, including their use for purposes beyond their original scope. The potential to further stigmatize, discriminate, exclude, and/or exploit vulnerable populations is vast. In doing so, these systems could seriously amplify allocative and representational harms (see Davis, Williams, and Yang 2021).

Concluding Remarks: A Motivation?

While various works have explored how AI systems may exhibit, reproduce, and/or augment inequities, more scholarship is needed on the role these systems play in current political-economic arrangements. This includes examinations of how global leaders—like China—may be exporting not only AI systems with extensive surveillance capabilities to other regimes, but the political know-how and securitizing logic necessary to abuse, misuse, and/or exploit them. The COVID-19 pandemic may offer the perfect guise for

these receiving entities to expand their AI-powered surveillance systems, in the process solidifying unequal power dynamics and eroding democratic ideals. This may alter the world order in extreme ways that particularly target marginalized and minoritized individuals and groups. These voices will be critical as we consider how best to address such potentiality. As it stands, we are woefully underprepared.

All this boils down to one thing—we must pay attention to what is happening in China.

References

Andersen, Ross. 2020. The Panopticon Is Already Here. *The Atlantic*, September. https://www.theatlantic.com/magazine/archive/2020/09/china-ai-surveillance/614197/ [accessed September 17, 2022].

Bhattacharya, Amar, David Dollar, Rush Doshi, Ryan Hass, Bruce Jones, Homi Kharas, Jennifer Mason, Mireya Solís, and Jonathan Stromseth. 2022. China's Belt and Road: The New Geopolitics of Global Infrastructure Development. *Brookings*, March 9. https://www.brookings.edu/research/chinas-belt-and-road-the-new-geopolitics-of-global-infrastructure-development/ [accessed September 20, 2022].

Corona-Warn-App. 2022. *Frequently Asked Questions about the Corona-Warn-App: Objectives*. https://www.coronawarn.app/en/faq/results/#objectives [Accessed December 2, 2022].

Chutel, Lynsey. 2018. China Is Exporting Facial Recognition Software to Africa, Expanding Its Vast Database. *Quartz*, May 25. https://qz.com/africa/1287675/china-is-exporting-facial-recognition-to-africa-ensuring-ai-dominance-through-diversity [accessed September 21, 2022].

Kurlantzick, Joshua. 2020. Accessing China's Digital Silk Road Initiative. *Council on Foreign Relations (CFR)*, December 18. https://www.cfr.org/china-digital-silk-road/ [accessed September 20, 2022].

Davis, Jenny L., Apryl Williams, and Michael W. Yang. 2021. Algorithmic Reparation. *Big Data & Society* 8 (2): 1-12. https://doi.org/10.1177/20539517211044808.

Dencik, Lina, Arne Hintz, Joanna Redden, and Emiliano Treré. 2019. Exploring Data Justice: Conceptions, Applications and Directions. *Information, Communication & Society* 22 (7): 873-881.

Foucault, Michel. 1978. *The History of Sexuality*. New York: Pantheon Books.

Gan, Nectar. 2020. With the coronavirus under control, this Chinese city wants to score and rank its residents based on their health and lifestyle. *Cable News Network (CNN),* May 25. https://www.cnn.com/2020/05/25/tech/hangzhou-health-app-intl-hnk/index.html [accessed August 11, 2022.

Habib, Benjamin and Viktor Faulknor. 2017. The Belt and Road Initiative: China's Vision for Globalisation, Beijing-style. *The Conversation*, May 16. https://theconversation.com/the-belt-and-road-initiative-chinas-vision-for-globalisation-beijing-style-77705 [accessed August 13, 2022].

Hanrieder, Tine and Christian Kreuder-Sonnen. 2014. WHO Decides on the Exception? Securitization and Emergency Governance in Global Health. *Security Dialogue* 45 (4): 331-348.

Hawkins, Amy. 2018. Beijing's Big Brother Tech Needs African Faces. *Foreign Policy*, July 24. https://foreignpolicy.com/2018/07/24/beijings-big-brother-tech-needs-african-faces/ [accessed August 13, 2022].

Kharpal, Arjun. 2020a. Coronavirus could be a "catalyst" for China to boost its mass surveillance machine, experts say. *CNBC*, February 24. https://www.cnbc.com/2020/02/25/coronavirus-china-to-boost-mass-surveillance-machine-experts-say.html [accessed August 11, 2022].

Kharpal, Arjun. 2020b. Use of surveillance to fight coronavirus raises concerns about government power after pandemic ends. *CNBC*, March 30. https://www.cnbc.com/2020/03/27/coronavirus-surveillance-used-by-governments-to-fight-pandemic-privacy-concerns.html [accessed August 11, 2022].

Malik, Yashpal Singh, Shubhankar Sircar, Sudipta Bhat, Mohd Ikram Ansari, Tripti Pande, Prashant Kumar, Basavaraj Mathapati, Ganesh Balasubramanian, Rahul Kaushik, Senthilkumar Natesan, Sayeh Ezzikouri, Mohamed E. El Zowalaty, and Kuldeep Dhama. 2021. How Artificial Intelligence May Help the Covid-19 Pandemic: Pitfalls and Lessons for the Future. *Reviews in Medical Virology* 31 (5): 1-11.

Morgan Stanley. 2018. Inside China's Plan to Create a Modern Silk Road. *Morgan Stanley*, March 14. https://www.morganstanley.com/ideas/china-belt-and-road [accessed September 20, 2022].

Mozur, Paul, Raymond Zhong, and Aaron Krolik. 2021. In Coronavirus Fight, China Gives Citizens a Color Code, with Red Flags. *The New York Times*, July 26. https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html [assessed September 17, 2022].

Parkinson, Joe, Nicholas Bariyo, and Josh Chin. 2019. Huawei Technicians Helped African Governments Spy on Political Opponents. *The Wall Street Journal*, August 15. https://www.wsj.com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents-11565793017 [accessed September 21, 2022].

Terry, Nicolas P. 2018. Big Data and Regulatory Arbitrage in Healthcare. In *Big Data, Health Law, and Bioethics*, edited by I. Glenn Cohen, Holly Fernandez Lynch, Effy Vayena, and Urs Gasser, 56-68. Cambridge, UK: Cambridge University Press.

Wong, Zoie S.Y., Jiaqi Zhou, and Qingpeng Zhang. 2019 Artificial Intelligence for Infectious Disease Big Data Analytics. *Infection, Disease & Health* 24 (1): 44-48.

Wong, Tess and BBC Chinese. 2022. Henan: China Covid app restricts residents after banking protests. *BBC News*, June 14. https://www.bbc.com/news/world-asia-china-61793149 [accessed August 11, 2022].

Zhao, Iris. 2022. Concerns over Beijing's plans to roll out digital health code system for every aspect of residents' health. *ABC News*, November 25. https://www.abc.net.au/news/2022-11-26/china-plan-for-national-digital-health-code-system/101690448 [accessed November 27, 2022].