Asian Journal of Comparative Law (2023), **18**, 91–115
doi:10.1017/asjcl.2022.31

ASIAN JOURNAL OF COMPARATIVE LAW
CAMBRIDGE UNIVERSITY PRESS

ARTICLE

Digital Surveillance Trends and Chinese Influence in Light of the COVID-19 Pandemic

Marco André Germanò[1*], Ava Liu[2**], Jacob Skebba[3***] and Bulelani Jili[4****]

[1]Peking University, China, and University of São Paulo, Brazil, [2]Harvard Law School, United States, [3]China, Law, and Development Project, University of Oxford. United Kingdom and [4]Harvard University, United States
Corresponding author. E-mail: marco.rgermano@gmail.com

(Received 6 April 2022; revised 15 August 2022; accepted 12 September 2022; first published online 23 January 2023)

Abstract

Countries across the world expanded digital surveillance strategies in response to the COVID-19 pandemic. As the pandemic occurred contemporaneously with a global trend toward greater digital repression, commentators advanced the notion that China would use the health crisis to promote a technology-enabled form of authoritarian governance abroad. This article surveys the evidence for these claims by first examining the literature on the increase of digital surveillance associated with China and then presenting three case studies from developing countries with varying responses to the COVID-19 pandemic. The selected countries – Brazil, South Africa and Vietnam – used surveillance technology as part of their pandemic response and have either been influenced by Chinese approaches or adopted Chinese technology in recent years. Examining these case studies allows us to better understand claims regarding China's role in the general spread of digital surveillance and the interplay between Chinese state objectives and local political environments. Crucially, we illustrate how China's engagement in digital governance abroad is heavily contingent on domestic environments. Against a backdrop of China's growing influence in global digital governance, the effects observed in these case studies of Chinese surveillance models and technology proliferating through pandemic management are diffuse and contextualised by local factors.

The COVID-19 Pandemic and Chinese Influence in Global Digital Surveillance

The emergence and subsequent spread of the SARS-CoV-2 virus led countries worldwide to implement a range of measures intended to protect their populations and economies from the COVID-19 pandemic. National response strategies varied in scope and proportionality from those focused on eliminating COVID-19 to those intended to suppress viral transmission or mitigate its effects.[1] While there has been debate about the efficacy of various strategies and the specific regulations

*Yenching Scholar, Peking University; LLM candidate, University of São Paulo; Research Assistant, Institute of Applied Economic Research (IPEA), Fundação Getulio Vargas (FGV) and the Federal University of Rio Grande do Sul (UFRGS); Research Associate at the University of Oxford. This article has benefitted from discussions within the China, Law and Development (CLD) project. The authors thank Matthew Erie and the CLD Research Associates for their comments on earlier drafts. The authors also thank Victoria Hayman for her contributions. All errors are the authors'.

**JD, Harvard Law School; LLM, University of Cambridge.

***JD, University of Wisconsin; Research Associate, China, Law, and Development Project, University of Oxford.

****PhD candidate and Meta Research PhD Fellow, Harvard University; Visiting Fellow, Yale Law School; Cybersecurity Fellow, Harvard Kennedy School; Fellow, Atlantic Council; Scholar-in-Residence, Electronic Privacy Information Center; Research Associate, Oxford University.

[1]Laura Spinney, 'How Elimination Versus Suppression Became Covid's Cold War' (The Guardian, 3 Mar 2021) <https://bit.ly/3p8SuW2> accessed 1 Dec 2022.

operationalising them,[2] it is notable that a myriad of surveillance tools and techniques were adopted on an unprecedented scale in an attempt to monitor the propagation of the virus.[3] These strategies encompassed several layers of technology, including new or improved approaches such as location-tracking apps, artificial intelligence (AI) devices, large-scale closed-circuit television (CCTV) networks, biometrics wearables, drones, and big data analytics.[4]

Debate and discussion around the role of technology and data in society, both within civil society and the scholarly community, predates the pandemic.[5] However, COVID-19 propelled the use of data-driven surveillance tools to a new level in many countries' public health strategies. In multiple jurisdictions, the health crisis precipitated incursions into citizens' personal data that had been unjustifiable before the pandemic. Many governments took extraordinary measures to control the spread of the virus as state officials tracked, collected, and analysed people's personal information, including data on their physical locations, beyond typical procedures of due process and state oversight.[6] Therefore, as pandemic response strategies were implemented, concerns about government-led surveillance were raised; fingers were pointed at states ranging from single-party autocratic regimes to more liberal constitutional democracies.[7]

The pandemic also came at the tail end of a decade that saw growing Chinese involvement in global digital infrastructure[8] – the very same digital infrastructure involved in many countries' pandemic responses. It is unsurprising, then, that pre-pandemic discussion of China's impact on international data governance has now given rise to a debate about China's influence on pandemic management and surveillance strategies abroad. With the background of a public health crisis operating as a legitimate reason and shroud for a significant increase in state surveillance, authors argued that the pandemic rendered a proof of concept as well as a political opportunity for the deployment of illiberal technologies related to China's repression model.[9] Others highlighted that China's pandemic response strategies could diffuse to other countries due to its major power status and global economic role.[10] From this vantage point, the global adoption of surveillance technologies

[2]See eg, The Lancet, 'Contact tracing: digital health on the frontline' (2020) 2 The Lancet Digital Health e561 <https://bit.ly/3h9KMXi> accessed 1 Dec 2022.

[3]Sera Whitelaw et al, 'Applications of digital technology in COVID-19 pandemic planning and response' (2020) 3 The Lancet Digital Health 435 <https://bit.ly/3p8PSHE> accessed 1 Dec 2022.

[4]For a comprehensive database of digital tracking and physical surveillance tools deployed around the world, see Samuel Woodhams, 'Covid-19 Digital Rights Tracker' (Top 10 VPN, 25 Mar 2021) <https://bit.ly/3t2WCI3> accessed 1 Dec 2022.

[5]See eg, Zeynep Tufekci, 'Engineering the public: Big data, surveillance and computational politics' (2014) 19 First Monday <https://bit.ly/3h9sd5C> accessed 1 Dec 2022; David Lyon, *Surveillance after Snowden* (Polity Press 2015); Shoshana Zuboff, *The Age of Surveillance Capitalism* (Public Affairs 2019)

[6]Adrian Shahbaz & Alie Funk, 'Freedom on the Net 2020: The Pandemic's Digital Shadow' (Freedom House, 2020) <https://bit.ly/3IeTa3s> accessed 1 Dec 2022.

[7]See eg, Steven Feldstein, *The Rise of Digital Repression: How Technology is Reshaping Power, Politics, and Resistance* (Oxford University Press 2021) 277–279 (showing that not only authoritarian governments but also liberal democracies pursued digital surveillance during the pandemic); Deborah Brown & Amos Toh, 'Technology is Enabling Surveillance, Inequality During the Pandemic' (Human Rights Watch, 4 Mar 2021) <https://bit.ly/3h9sTba> accessed 1 Dec 2022 (finding that government reliance on intrusive technologies with risky outcomes to human rights has also been the case in several liberal democracies).

[8]See eg, Richard Ghiasy & Rajeshwari Krishnamurthy, 'China's Digital Silk Road and the Global Digital Order' (The Diplomat, 13 Apr 2021) <https://bit.ly/3p7yhQp> accessed 1 Dec 2022.

[9]See eg, Lydia Khalil, 'Digital Authoritarianism, China and Covid' (Lowy Institute Analysis, 2 Nov 2021) <https://bit.ly/3JQWO4d> accessed 1 Dec 2022; Sheena C Greitens, 'Surveillance, Security, and Liberal Democracy in the Post-Covid World' (2020) 74(S1) International Organization E169; Aidan Powers-Riggs, 'Covid-19 is Proving a Boon for Digital Authoritarianism' (Center for Strategic and International Studies, 17 Aug 2020) <https://bit.ly/3LV2QCw> accessed 1 Dec 2022; Emily de La Bruyère & Nathan Picarsic, 'China's next plan to dominate international tech standards' (TechCrunch, 11 Apr 2020) <https://tcrn.ch/35lbRE3> accessed 1 Dec 2022.

[10]See Greitens (n 9) E174–E178 and E186–E187 (arguing that the CCP could eventually spread its model of pandemic response abroad, although diffusion was not a foregone conclusion).

https://doi.org/10.1017/asjcl.2022.31 Published online by Cambridge University Press

and practices would be a consequence of China's ambitions to promote its leadership in the digital realm, ultimately shifting how states conduct the business of governance.[11]

Notwithstanding these claims, other scholars have challenged the idea that China is intentionally exporting some form of digital authoritarianism.[12] Gagliardone notes that China's supply factors may encourage the proliferation of technologies that have adverse consequences; however, evidence is lacking to support assertions on its intention to promote surveillance overseas.[13] Similarly, Matthew Erie and Thomas Streinz propose conceptualising China's influence in digital infrastructure abroad through a 'Beijing Effect'. Namely that China's impact on both governance and development is created through demand and supply-side factors.[14] These interpretations challenge the notion that the international adoption of technology for illiberal purposes is influenced by the Chinese Communist Party (CCP) state security objectives and alleged desire to re-shape global governance.[15]

This article attempts to contribute to the ongoing debate about China's role in the global spread of digital surveillance as well as claims regarding China's role in the rise of digital repression. We do so by examining technology and data use in managing the pandemic across three jurisdictions that show growing links with Chinese information and technology (ICT) companies and that have experienced a rise in digital surveillance in recent years: Brazil, South Africa, and Vietnam. To this end, we use the COVID-19 pandemic as an analytical framework, as it has been a particular circumstance in recent global history where governments and populations favored technological surveillance as a way to manage the advance of the virus.[16]

Through our cases, we compare the deployment of such surveillance practices in light of the pandemic and explore whether and how China could influence the spread and governance of such strategies.[17] We observe that the increase in digitally intrusive strategies during the pandemic has been primarily linked to domestic predilections in our sample, such as each countries' institutional features, political capacity to employ large-scale surveillance systems, and their own interests in replicating Chinese surveillance models or engaging with its technology companies. Thus, we contend that simplistic claims linking the use of Chinese technology to the increase in digital surveillance generally depict a causal relation that is not necessarily confirmed in practice. Instead, we argue that the pandemic illustrates there can be little correlation between the adoption of Chinese surveillance technology and the erosion of democratic institutions or civil liberties *per se* – yet this

[11]See Emily de La Bruyère, 'A New Type of Geopolitical Power: China's Competitive Strategy for the Digital Revolution', in Emily de La Bruyère, Doug Strub & Jonathon Marek (eds), *China's Digital Ambitions: A Global Strategy to Supplant the Liberal Order* (National Bureau of Asian Research, Mar 2022).

[12]See eg, Christopher Walker, Shanthi Kalathil & Jessica Ludwig, 'The Cutting Edge of Sharp Power' (2020) 31 Journal of Democracy 124, 129–132; Jessica Chen Weiss, 'Understanding and Rolling Back Digital Authoritarianism' (War on the Rocks, 17 Feb 2020) <https://bit.ly/3IbEVN6> accessed 1 Dec 2022.

[13]Iginio Gagliardone, 'The Impact of Chinese Tech Provision on Civil Liberties in Africa' (South African Institute of International Affairs, Policy Insights 99, Dec 2020) <https://bit.ly/3t1sgG8> accessed 1 Dec 2022.

[14]Matthew S Erie & Thomas Streinz, 'The Beijing Effect: China's 'Digital Silk Road' as Transnational Data Governance' (2021) 54 New York University Journal of International Law and Politics 3.

[15]See Samantha Hoffman, 'China's Tech-Enhanced Authoritarianism: Testimony before the House Permanent Select Committee on Intelligence, Hearing on "China's Digital Authoritarianism: Surveillance, Influence, and Political Control"' (16 May 2019) <https://bit.ly/3v5N7e5> accessed 1 Dec 2022 (advancing the idea that the CCP is deliberately seeking to influence data governance models abroad due to its state objectives).

[16]See eg, Anna Wnuk, Tomasz Oleksy & Dominika Maison, 'The acceptance of Covid-19 tracking technologies: The role of perceived threat, lack of control, and ideological beliefs' (2020) 15(9) PLoS One <https://bit.ly/3IeO2wv> accessed 1 Dec 2022 (a case study showing how the pandemic has positively shifted perceptions of surveillance technologies among Polish citizens).

[17]Since the COVID-19 outbreak in late 2019, states have dramatically strengthened their surveillance tools and techniques mainly through partnerships with private companies selected within a global market notably characterised by the presence of Chinese technology companies. See eg, Steven Feldstein, 'The Global Expansion of AI Surveillance' (Carnegie Endowment for International Peace, 17 Sep 2019) <https://bit.ly/3Hj0SbS> accessed 1 Dec 2022.

https://doi.org/10.1017/asjcl.2022.31 Published online by Cambridge University Press

relationship may still be noted to play out around factors made available in local contexts, which we explore in our three case studies. We conclude by highlighting that insofar there is growing evidence showing Chinese ambitions to influence data governance models and surveillance practices globally,[18] such influence in times other than a pandemic needs to be seriously evaluated against local driving factors. These local conditionalities structure China's technological engagement abroad and play a significant role in potentially adverse outcomes such as increased digital repression and digitally empowered authoritarianism.

There are two methodological caveats to this research. First, our case studies are useful for disentangling discernible trends of international discourses about China's role in the spread of digital surveillance; nevertheless, they should be assessed together with other works that examine the topic through different angles and countries from our own.[19] Our main goal herein is not to provide absolute conclusions about the role of China in the global spread of digital surveillance. Rather, we aim to illuminate and contextualise narratives around Chinese companies providing surveillance infrastructure to developing nations. Second, further research to evaluate the correlation between Chinese influence and the rise of digital surveillance may take different approaches.[20] Our own approach, examining closely the experiences of countries in their interaction with China and how their uptake of surveillance strategies was formed, show that countries demonstrate divergent experiences shaped by traceable developments in their own domestic trajectory and intentional choices to engage with China. These accounts highlight nuanced aspects of relevance to studies on Chinese surveillance technology and models proliferating abroad.

The article is divided into three sections in addition to this introduction and its conclusion. First, we examine the aforementioned discussions regarding China's influence on digital repression and governance abroad. Then, we present the case studies on Brazil, South Africa, and Vietnam, comparing how each of these countries applied distinct pandemic responses and to what extent they used Chinese technology or were influenced by Chinese approaches to pandemic management surveillance. Finally, we analyse whether and how China's digital surveillance model is spreading to other countries. We also put forward some considerations and further research questions on how China could effectively exert influence on data management abroad.

Interpreting China's Role in the Global Spread of Digital Surveillance

Over the past few decades, the densification of digital infrastructure and the exponential increase in internet bandwidth has enabled an ever-growing amount of data to be collected, processed, and stored around the world.[21] Through these technological foundations, the world has witnessed an emerging raft of surveillance practices surrounding new digital tools and techniques, which have significantly transformed how governments and private enterprises wield data for enhanced state control and economic data-driven applications.[22]

[18]See generally de La Bruyère, Strub & Marek.

[19]See eg, Iginio Gagliardone, *China, Africa, and the Future of the Internet* (Zed Books 2019) (analysing Chinese ICT companies engagement with Africa); Erie & Streinz (n 14) 63–83 (presenting a case study on the impacts of China's DSR on Pakistan, including aspects of digital surveillance); Feldstein (n 7) chs 4, 5, and 6 (examining Chinese digital repression in Thailand, Ethiopia, and the Philippines); Joshua Kurlantzick et al, 'Assessing China's Digital Silk Road Initiative' (Council on Foreign Relations, 18 Dec 2020) <https://on.cfr.org/3HfC4Bg> accessed 1 Dec 2022 (highlighting aspects of Chinese investments in digital infrastructure in Ecuador, Egypt, Myanmar, Pakistan, Serbia, Zambia, and Zimbabwe).

[20]An example being large-n analyses evaluating the statistical correlation of Chinese exports and technology presence with measurements of the erosion of democratic institutions.

[21]Rob Kitchin, *The Data Revolution: Big Data, Open Data, Data Infrastructures & their Consequences* (SAGE Publications 2014) (examining how the data landscape is rapidly changing with remarkable social, political and ethical consequences).

[22]See eg, Cloves Norris & Dean Wilson (eds), *Surveillance, Crime and Social Control* (Routledge 2006) <https://bit.ly/3va3pm> accessed 1 Dec 2022 (exploring how new digital technologies that enhance data collection and processing are ultimately changing the political economies of societies); Dan Ciuriak, 'The Economics of Data: Implications for the Data-Driven

https://doi.org/10.1017/asjcl.2022.31 Published online by Cambridge University Press

While not the first protagonist of these surveillance trends,[23] China has come to attract global attention for its companies' growing prominence in producing such digital technologies. In the last decade, firms such as China Mobile, China Unicom, China Telecom, Huawei, ZTE, Hikvision and Dahua have become global leaders in the ICT market, offering diverse solutions to national and international consumers.[24] Concurrent with the advance of Chinese companies, the world has also experienced a rise in digital repression as global internet freedom has been continuously declining and several countries have adopted censorship mechanisms and automated surveillance systems.[25] Based on these observations, commentators began to highlight China's role in this process as the ultimate model of political repression and the go-to supplier for authoritarian regimes seeking to shore up domestic control.[26] Thus, when the first human infection of COVID-19 was confirmed in Wuhan, China was already in the spotlight for its growing role in deploying surveillance mechanisms at home and abroad.

Although some of the concerns about the Chinese government and companies providing surveillance tools to other countries seem well-founded, the real picture of whether and how China has been pushing its governance model to other countries is not as clear as critics usually suggest. In this section, we juxtapose two of the primary academic interpretations of how China could be exerting international influence to reshape global norms and standards in ways that enable authoritarian behaviour in the digital realm. First, we present the claims on how China is strengthening digital surveillance abroad in advancing its 'techno-authoritarian' political model by transplanting technology-based enablers of repressive rule. Then, we look at the literature that examines China's influence through a more complex framework of interactions between local and international factors.

China Exporting Digital Authoritarianism

'Digital authoritarianism' is broadly defined as the use of digital information technology by authoritarian regimes to surveil, repress, and manipulate domestic and foreign populations.[27] The conceptual narrative highlights how illiberal governments have been increasingly using technology-driven playbooks for authoritarian rule – the most notorious contemporary example being China itself.[28]

Economy', in Centre for International Governance Innovation, 'Data Governance in the Digital Age' (5 Mar 2018) <http://dx.doi.org/10.2139/ssrn.3118022> accessed 1 Dec 2022 (arguing that the new data-driven economy has distinct characteristics of previous economic systems, with relevant impacts to the design of regulatory frameworks).

[23]Didier Bigo, 'Digital Surveillance and Everyday Democracy', in Leanne Weber, Elaine Fishwick & Marinella Marmo (eds), *The Routledge International Handbook of Criminology and Human Rights* (Routledge 2007) 125–135 (describing the political and technological context of how surveillance practices became increasingly common in modern societies, with a particular attention on the role of the United States' government and companies).

[24]Australian Strategic Policy Institute (ASPI), 'Mapping China's Tech Giants' (2021) <https://chinatechmap.aspi.org.au/#/map> accessed 20 Feb 2022 (showing how Chinese ICT companies have spread across a considerable part of the world).

[25]Global internet freedom has been declining since 2010 and China still ranks as the worst environment for internet freedom. See Adrian Shahbaz & Allie Funk, 'Freedom on the Net 2021: The Global Drive to Control Big Tech' (Freedom House, 2021) <https://bit.ly/3BGB73Z> accessed 1 Dec 2022.

[26]See eg, Stanford Cyber Policy Center, 'Countering the Rise of Digital Authoritarianism, China, AI, and Human Rights' (Nov 2020) <https://bit.ly/3t1fqYd> accessed 1 Dec 2022; US Senate Democratic Staff, 'The New Big Brother: China and Digital Authoritarianism' (Committee on Foreign Relations United States Senate, 21 Jul 2020) <https://bit.ly/3BIxsCG> accessed 1 Dec 2022; Tiberiu Dragu & Yonatan Lupu, 'Digital Authoritarianism and the Future of Human Rights' (2021) 75 International Organization 991; Alina Polyakova & Chris Meserole, 'Exporting digital authoritarianism: The Russian and Chinese models' (Brookings, Aug 2019) <https://brook.gs/35isUH9> accessed 1 Dec 2022; The President of the United States, 'United States Strategic Approach to the People's Republic of China' (2020) 5 <https://bit.ly/3H5zw8Z> accessed 1 Dec 2022.

[27]ibid.

[28]See eg, Xiao Qing, 'Chinese Digital Authoritarianism and Its Global Impact' 43 POMPEPS Studies 35 <https://bit.ly/3IsOyHr> accessed 1 Dec 2022; James Leibold, 'Surveillance in China's Xinjiang Region: Ethnic Sorting, Coercion, and Inducement' (2020) 29 Journal of Contemporary China 46 <https://bit.ly/3I8saCO> accessed 1 Dec 2022.

https://doi.org/10.1017/asjcl.2022.31 Published online by Cambridge University Press

While the dangers to civil liberties to those living in China seem evident, the claim of its role in transplanting digital authoritarianism to other jurisdictions is less clear.

The claim first relates to the economic activities of different Chinese companies providing digital tools with advanced surveillance capabilities to governments with poor human rights records. Among the most ubiquitous technologies are advanced facial-recognition software, safe city projects, and data-analytic tools. Some actors argue, inter alia, that Chinese technology is embedded with a malign governance model that allows substantial information collection and tracking, strengthening government overreach while reducing domestic freedom.[29] Crucially, these positions generally suppose a Chinese strategy to promote its normative values through a coordinated effort between the CCP and corporate actors, whether state-owned or (formally) private;[30] an example being the recent accusations that Huawei, as an agent tied extensively with the Chinese state, has pitched products and services for its surveillance solutions, acting in coordination with the CCP's agenda.[31] Additionally, commentators highlight how China's technology exports have been fuelling illiberal regimes through the support of its financial institutions – which are touted to be less intrusive than Western organisations.[32] Thus, as Chinese companies peddle its products with little or no conditionalities on domestic policies, they become particularly attractive for authoritarian regimes barred from global financial markets.[33]

Second, authors argue that China's major power status and its leadership in international organisations could help diffuse its 'model' to other countries, as China's example creates permissive conditions for authoritarian regimes to enhance their repressive capacity.[34] Under this logic, other governments would be encouraged to replicate China's apparatus of repression, whether due to Chinese financial support or indirect political allowances. This process would also entail a cross-border regulatory effect. As China accesses new markets, ones with allegedly weak regulatory frameworks, it helps push forward new rules in domestic jurisdictions on digital rights, privacy, and data collection, through emulation and modelling.[35] To this end, critics underscore how Chinese companies have been hosting officials from a number of countries for periodic training on its sprawling system of censorship and surveillance,[36] and how Chinese companies also face pressure from the Chinese government to spy, sabotage, or take other actions on its behalf, making global data more accessible to Chinese intelligence agencies through both legal and extra-legal methods.[37]

[29]See text and sources cited in (n 26).

[30]See eg, Lindsay Maizland & Andrew Chatzky, 'Huawei: China's Controversial Tech Giant' (Council on Foreign Relations, 6 Aug 2020) <https://on.cfr.org/3s95YmA> accessed 1 Dec 2022 (describing the influence from the Chinese party-state on Huawei).

[31]Eva Dou, 'Documents link Huawei to China's surveillance programs' (The New York Times, 14 Dec 2021) <https://wapo.st/3VYxvmU> accessed 1 Dec 2022.

[32]Axel Dreher et al, 'Aid, China, and Growth: Evidence from a New Global Development Finance Dataset' (AidData Working Paper no 46, 10 Oct 2017) <https://bit.ly/3BKF8Va> accessed 1 Dec 2022 (finding that Chinese financial aid is usually less concessional and more commercially-oriented than those from Western donors and lenders).

[33]Steven Feldstein, 'Testimony before the U.S.-China Economic and Security Review Commission: Hearing on China's Strategic Aims in Africa' (8 May 2020) 9–10 <https://bit.ly/3hclYBr> accessed 1 Dec 2022.

[34]Greitens (n 9) E180.

[35]Feldstein (n 7) 48–55.

[36]Benjamin Tsui, 'Do Huawei's Training Programs and Centers Transfer Skills to Africa?' (China Africa Research Initiative Policy Brief no 14, Jul 2016) <https://bit.ly/3paEgUF> accessed 1 Dec 2022 (explaining Huawei's efforts to train local workforce on ICT matters in Africa); Adrian Shahbaz, 'The Rise of Digital Authoritarianism – Freedom of the Net 2018' (Oct 2018) 2–10 <https://bit.ly/36yj6JD> accessed 1 Dec 2022 (highlighting that representatives from at least 36 countries have attended Chinese trainings and seminars on media and information management in the last decade).

[37]See Maizland & Chatzky (n 30); Maya Wang, 'China's Techno-Authoritarianism Has Gone Global' (Foreign Affairs, 8 Apr 2021) <https://fam.ag/3LQosjv> accessed 1 Dec 2022 (arguing that the Chinese government is gaining influence on global data due to unclear legal limits to state control over its multinational companies).

https://doi.org/10.1017/asjcl.2022.31 Published online by Cambridge University Press

Although other authoritarian governments, such as Russia and Saudi Arabia, have also been exploiting the surveillance toolkit for their own purposes,[38] China, according to some, arguably plays a greater role in this trend as its companies have been a major driver for the expansion of surveillance tools worldwide. Since 2008, at least 80 countries have adopted public security technologies and surveillance platforms from Chinese companies.[39] The customer profile is varied, including emerging as well as developed nations.[40] The fact that other European, North American, and Asian companies provide the same technology is overshadowed by the fact that their market share in surveillance solutions is much smaller than that of Chinese companies.[41]

While it seems clear that digital authoritarianism as a narrative accurately describes several worrying trends in the employment of digital technologies, the approach seems to exaggerate the degree to which China has been actively transplanting governance approaches on surveillance tools and techniques to other jurisdictions. In particular, many scholars appear to agree that the argument of China pushing digital authoritarianism in other countries is oversimplified.[42] Instead, a model acknowledging demand-side drivers in addition to supply-side factors might better explain China's influence on other countries concerning the adoption of digital technologies and the conditions of their use.

China's Influence in Global Digital Surveillance: A Two-Fold Narrative

Current media, state, and academic discourses speculate about coordinated efforts between the Chinese state and private actors to promote digital surveillance practices abroad. Even though this remains a valid hypothesis, the speculation emphasises the fact that Chinese supply factors prompt the proliferation of governance and surveillance technology. In this light, the CCP would be willing to assert a Chinese-based vision of digital governance in other jurisdictions. Some scholars, however, raise critical questions about how we should interpret China's adaptive posture and its willingness to meet foreign actors in their often-unique circumstances.

Gagliardone, for instance, provides a measured account of Beijing's growing geopolitical footprint. He argues that as Beijing expands access to digital infrastructure in Africa, the means of its ICT system also imply political processes available in local contexts. The proclivity to technically and financially support state actors regardless of their legal environments and political regime type raises questions about how China negotiates differences. More to the point, this conception of a locally responsive China does not necessarily negate complicity in adverse outcomes on the ground – like unwarranted surveillance. Rather, it points to how we should examine local and global features as interconnected vectors.

This reading is strengthened by Erie and Streinz. While not the first commentators to describe China's influence through a push/pull framework,[43] these authors employ this interpretation in articulating the theory of what they term the 'Beijing Effect.'[44] This term appears deliberately chosen

[38]See eg, Laura HC Howells, 'Digital Authoritarianism in China and Russia: A Comparative Study' (Honors thesis, Bowdoin College 2021) <https://bit.ly/3Isy3et> accessed 1 Dec 2022; Afef Abrougui, 'Digital Authoritarianism in the GCC and its Broader Regional Consequences' (Carnegie Endowment for International Peace, 19 Oct 2021) <https://bit.ly/3v9OtnX> accessed 1 Dec 2022.

[39]Sheena Chestnut Greitens, 'Dealing with Demand for China's Global Surveillance Exports' (Brookings, Apr 2020) 2 <https://brook.gs/3BGaT1k> accessed 1 Dec 2022.

[40]ASPI (n 24).

[41]One of the reasons given for this broad market is that the price difference of Chinese surveillance equipment can be 10 times smaller than some of its competitors. For example, Axis' cameras (Sweden) cost an average of USD 372, while Hikvision's cameras cost around 37 USD. See later Gordon (n 95).

[42]See eg, Greitens (n 9); Feldstein (n 7); Erie & Streinz (n 14).

[43]Chinese influence on technology governance abroad was discussed within a push/pull framework at least as early as April 2020. See Greitens (n 39) 5–6.

[44]Erie & Streinz (n 14).

https://doi.org/10.1017/asjcl.2022.31 Published online by Cambridge University Press

to contrast with the 'Brussels Effect', a term describing instead how Europe influences governance and corporate behaviour abroad through European Union (EU) regulation and standardisation.[45] Speaking specifically with respect to technology governance, the 'Beijing Effect' argues that China develops and exercises influence through a combination of demand-side and supply-side factors, an approach less overtly legalistic compared to the EU and United States' (US) propensity for exercising influence through extraterritorial application of regulation or formal legal instruments.[46] Pull, or demand-side, factors include emerging countries' desire for affordable digital development as well as a desire to retain control over domestic and cross-border data flows.[47] On the other hand, push, or supply-side, factors include China's activities to promote its technology and, to some extent, its approach to governance in international fora or through global development initiatives such as the Digital Silk Road.[48]

The 'Beijing Effect' theory refines more general theories regarding China's influence on technology governance abroad, but it does so primarily for a narrower set of technology use cases than are frequently discussed in the digital repression literature. In this regard, other scholars expand the forms digital authoritarianism may take. For example, Steven Feldstein provides a relatively comprehensive treatment of what he refers to as 'digital repression',[49] creating a taxonomy of the forms in which such repression appears. Feldstein divides digital repression into five practices, namely, surveillance, censorship, social manipulation and disinformation, internet shutdowns, and persecution of individuals for online activity. Feldstein argues, however, that there is not much evidence that other countries are adopting repressive digital tools and techniques because China is allegedly pushing them.[50] Rather, other factors better explain which governments engage in digital repression and which methods they use to do so. Feldstein specifically mentions the role of political environments, intelligence and security capacity, and levels of social media penetration in host nations.[51]

Answering whether China is exporting not only technology but also its values and governance approach requires further consideration of what 'export' entails. Scholars like Alden and Alves contend that China's technology and technical support does not mean categorical exportation of its normative values.[52] Instead, they contend that Beijing helps amplify domestic-led processes already present in local environments. Likewise, Gagliardone, Erie and Streinz, and Feldstein all argue convincingly that the notion of the exportation of values does not hold up under an interpretation of intentional pressure by China for other countries to adopt its approach to technology and data governance. This view, however, is contrasted by other authors, such as Emily de La Bruyère, Samantha Hoffman and Nigel Cory, who see in the Chinese government's policies and statements ambitions to promote a model of state controlled and delimited cyberspace.[53] According to their reading, the

[45]For more detailed discussion of the Brussels Effect, see Anu Bradford, 'The Brussels Effect' (2012) 107 Northwestern University Law Review 1 (posing that companies gravitate towards European law even when they are not legally required to do so due to the EU's major global status, benefits of global regulatory uniformity and high economic costs for non-compliance).

[46]Erie & Streinz (n 14) 26–31.

[47]ibid.

[48]ibid. See also Jonathan E Hillman, 'Statement before the U.S.-China Economic Security Review Commission: A "China Model?" Beijing's Promotion of Alternative Global Norms and Standards' (13 Mar 2020) <https://bit.ly/3HbO072> accessed 1 Dec 2022 (arguing that China's promotion of alternative global norms and standards happens in a three-fold process: creating alternative institutions, working within existing institutions, and promoting its own global development initiatives).

[49]Feldstein chooses to use the term 'digital repression' rather than 'digital authoritarianism' as he notes that repressive tools and techniques are not used exclusively by authoritarian regimes. See Feldstein (n 7) 25.

[50]Feldstein (n 7) 14; 273–277.

[51]ibid.

[52]Chris Alden & Cristina Alves, 'History & identity in the construction of China's Africa policy' (2008) 35 Review of African Political Economy 43, 43–45.

[53]Samantha Hoffman, 'Securing the Foundation: Building the Physical Infrastructure of the Digital World', in Emily de la Bruyère, Doug Strub & Jonathon Marek (eds), *China's Digital Ambitions: A Global Strategy to Supplant the Liberal Order* (National Bureau of Asian Research, Mar 2022) 11–22; Emily La Bruyère, 'Setting the Standards: Locking in China's

https://doi.org/10.1017/asjcl.2022.31 Published online by Cambridge University Press

CCP is strategically and deliberately rewriting the international digital architecture to shape the emerging global governance regime to closer align with Beijing's social and political values. This is precisely happening as the party-state increasingly controls cross-border data flows and influences the adoption of international norms, standards, and new digital infrastructure in other parts of the world.

In light of this debate, case studies on the use of Chinese technology in managing the pandemic in various jurisdictions can shed light on patterns in such technology and data use and, therefore, provide material for conclusions regarding China's influence on the adoption and governance of digital surveillance in other countries.

Digital Surveillance During the COVID-19 Pandemic: Case Studies on Brazil, South Africa, and Vietnam

As COVID-19 spread around the world, many countries were driven to systematically roll out or extend an array of digital measures of unprecedented scale and intrusiveness. Between February 2020 and March 2021, at least 80 countries in the world had employed some sort of surveillance strategy in their quests to track COVID-19 infections.[54] Such surveillance took a myriad of forms, from governments using digital applications to chart the virus' trajectory from broad swaths of personal data to physical infrastructure monitoring quarantine compliance.[55] In times of a pandemic, the use of digital tools with surveillance capabilities was greatly excused by public opinion, pushing government practice beyond legal and ethical boundaries.[56] Thus, the rapid embracing of such technologies and their opaque operational mechanisms promptly sparked debates about the impact on privacy and the need for proper oversight.[57] If technology was already being used with growing implications to human rights, the pandemic catalysed this process, raising concerns about the extent and limits of public and private overreach.

This was the case of China's own pandemic response, the first country to detect COVID-19 and to implement a large-scale panoptic strategy to prevent contagion.[58] The health strategy adopted by China is a paradigmatic case that illustrates the potential and challenges arising from the use of digital infrastructure in the face of a public crisis of the magnitude of COVID-19. China's case is also relevant for our analysis as it shows how the country pursued a strategy made available by a particular entanglement between the Chinese party-state, Chinese technology companies, and Chinese society – a distinct relationship that constrained partner countries attempting to replicate China's surveillance approach to COVID-19.[59]

Although the success of China's pandemic response has been associated with strict lockdowns, mass testing, and isolation protocols based on its previous responses to the 2002 severe acute respiratory syndrome (SARS) outbreak, digital surveillance tools were extensively used to

Technological Influence', in Emily de la Bruyère, Doug Strub & Jonathon Marek (eds), *China's Digital Ambitions: A Global Strategy to Supplant the Liberal Order* (National Bureau of Asian Research, Mar 2022) 49–72; Nigel Cory 'Writing the Rules: Redefining Norms of Global Digital Governance', in Emily de la Bruyère, Doug Strub & Jonathon Marek (eds), *China's Digital Ambitions: A Global Strategy to Supplant the Liberal Order* (National Bureau of Asian Research, Mar 2022) 73–88.

[54]See Woodhams (n 4).

[55]Reports highlight that at least 120 contact tracing apps were developed in 71 countries, while 20 governments have undertaken measures to collect data from mobile networks. See Woodhams (n 4).

[56]Bethania de Araujo Almeida et al, 'Personal data usage and privacy considerations in the COVID-19 global pandemic' (2020) 25 Ciência & Saúde Coletiva [Science and Public Health] 2487 <https://bit.ly/35leuWr> accessed 1 Dec 2022.

[57]Human Rights Watch, 'Joint Civil Society Statement: States use of digital surveillance technologies to fight pandemic must respect human rights' (2 Apr 2020) <https://bit.ly/3sb6FM1> accessed 1 Dec 2022.

[58]Emily Weinstein, 'China's Use of AI in its COVID-19 Response' (Center for Security and Emerging Technology, Data Brief, Aug 2020) <https://bit.ly/3VVqdjv> accessed 1 Dec 2022.

[59]Alex Jingwei He, Yuda Shi & Hongdou Liu, 'Crisis governance, Chinese style: distinctive features of China's response to the to the Covid-19 Pandemic' (2020) 3 Policy Design and Practice 242.

https://doi.org/10.1017/asjcl.2022.31 Published online by Cambridge University Press

complement these measures.[60] Prominent strategies included the processing of telecommunications networks data through smartphone apps – specifically the Alipay Health Code[61] – as well as new layers of technologies such as the use of drones, biometric wearables, and big data analytics.[62] After the first cases were registered in the country, China was able to build new data surveillance tools at a quick pace by leveraging existing e-technology and data surveillance infrastructure while tapping into its close relations between the state and private sectors.[63] China's response system was rather unique in this aspect as it collected new data by adding new health surveillance infrastructure to existing networks, rather than creating novel systems or using established data streams.[64] While some tools resembled examples seen internationally, others have gone a step further, expanding, for instance, the national authorities' reach over citizens' private messages.[65]

Examining China's particular pandemic response reveals characteristics which suggest less coherent intentionality or transferability to different regimes given that China's health digital surveillance model developed within its own system with certain Chinese characteristics. In particular, the development of its strategy came up through endorsed competitive evolution from local governments and relied heavily on existing public-private collaboration between the state and technology companies such as Alibaba and Tencent, which had already built out an existing digital application infrastructure. Therefore, China's response was characterised by a local government-focused ground-up approach rather than a coordinated central approach strategised from Beijing,[66] which seems to reduce the opportunity for intentional transplantation to partner countries.

While China's context shows limited evidence of intent to correspondingly influence other countries' pandemic response, its technology exports prior to the pandemic led commentators to argue that not only the crisis would accelerate the spread of digital repression, but it would also fuel China's drive to export surveillance practices to other jurisdictions.[67] In this section we analyse these claims in the face of three case studies that highlight how different governments with growing links to the Chinese government and companies coped with the COVID-19 health crisis. To this end, we examine publicly available documents on how digital surveillance strategies were modelled in Brazil, South Africa, and Vietnam – three counties that have used Chinese technology as part of

[60]See eg, Rob Kitchin, 'Civil liberties or public health, or civil liberties and public health? Using surveillance technologies to tackle the spread of COVID-19' (2020) 24 Space and Polity 362; Weinstein (n 58); 'To curb covid-19, China is using its high-tech surveillance tools' (The Economist, 27 Feb 2020) <https://econ.st/3JNJkWI> accessed 1 Dec 2022.

[61]One of the most notable public-private collaborations was the 'Alipay Health Code' application, introduced as a project of the local government of Hangzhou in February 2020, with the help of Ant Financial, and latter officially endorsed by the State Council. The application connects to local government's platforms and automatically tracks and updates users' information in real time by surveilling their social network and mobility data, and tracking users' interaction with other high-risk individuals and their past visits to areas defined as high-risk. Users that use the app through WeChat and Alipay do so by obtaining a code that registers their account with local authorities, including connecting facial recognition technology. See '全国版健康码，来了！ [The national health code is here!]' (Alipay, 16 Feb 2020). <https://mp.weixin.qq.com/s/amB7fBxLw8KSR9DcUsbTWg> accessed 1 Dec 2022.

[62]"To curb covid-19, China is using its high-tech surveillance tools' (n 60).

[63]Weinstein (n 58).

[64]Several countries known for extensive surveillance in managing the pandemic relied on such pre-existing, often commercial, data streams. Israel and Pakistan, for instance, repurposed counterterror tools that analyse mobile location meta-data records from data already being generated by telecommunications networks. South Korea also extensively used pre-existing data streams from mobile phone records and electronic payments data. See, respectively, Moran Amit et al, 'Mass-surveillance technologies to fight coronavirus spread: the case of Israel' (2020) 26 Nature Medicine 1167; Zuha Siddiqui, 'Pakistan Is Using a Terrorism Surveillance System to Monitor the Pandemic' (Slate, 15 Jul 2020) <https://bit.ly/3LStzzL> accessed 1 Dec 2022; Justin Fendos, 'How surveillance technology powered South Korea's COVID-19 response' (Brookings, 29 Apr 2020) <https://brook.gs/3P9n3q8> accessed 1 Dec 2022.

[65]Qianer Liu et al, 'China, Coronavirus and Surveillance: the Messy Reality of Personal Data' (Financial Times, 2 Apr 2020) <https://on.ft.com/3BKFHhK> accessed 1 Dec 2022.

[66]Marcella Siqueira Cassiano, Kevin D Haggerty & Ausma Bernot, 'China's Response to the COVID-19 Pandemic: Surveillance and Autonomy' (2021) 19 Surveillance & Society 94.

[67]See text and sources cited in (n 9).

https://doi.org/10.1017/asjcl.2022.31 Published online by Cambridge University Press

their pandemic response or have been influenced by Chinese surveillance approaches in recent years.

The case studies offered here represent complementary but distinct political contexts. Brazil and South Africa are regarded as flawed democracies, while Vietnam has an authoritarian government.[68] In recent years, all three countries have witnessed the growing involvement of Chinese ICT companies in their markets as they provide telecommunications hardware and software to governments agencies and private actors, often outcompeting technology companies from the US and Europe. Paralleled to this emergence, the three countries have also watched a decline in the quality of democracy[69] and internet freedom,[70] and, in the case of Brazil and Vietnam, a rise in digital repression indicators.[71] Thus, the three case studies together present a diverse analytical scenario where Chinese digital surveillance technology and techniques are being deployed against a scenario of diminishing democratic standards.

Brazil

The use of digital strategies has been a remarkable element in Brazil's pandemic response. Since the outbreak of COVID-19, public authorities have implemented a variety of technologies to coordinate health actions and enforce quarantine mandates.[72] The most relevant technologies employed at the national level included developing a contact-tracing application, collecting data from telecommunications networks, installing AI-empowered facial recognition cameras (FRC) in public and private venues, and using drones. Chinese companies were not directly involved in these efforts; however, a large part of Brazil's pandemic strategy relied on technology deployed by them in the country before and during the pandemic.

The first guidelines for the Brazilian pandemic response were framed in *Law No 13,979*, a legislation that was approved in early February 2020.[73] Through this enactment, the Brazilian government granted its Ministry of Health broad powers to deal with the public health emergency with the aim of preventing the spread of COVID-19. For this purpose, the law mandated the recording of data of confirmed and suspected individuals, and the sharing of essential personal data to government agencies for their respective identification. All data collected has been stored in the National Network of Health Data (*Rede Nacional de Dados em Saúde* or RNDS), a database created in May 2020 and controlled by the federal government.[74]

After Brazil's parliament approved the law, discussions in the Brazilian national government emerged around creating a large-scale surveillance platform to trace infections. Jair Bolsonaro's administration then formulated two main strategies: (i) ordering private telecommunications companies to share user data with government entities and (ii) developing a national contact-tracing application. However, during the course of the pandemic, the Brazilian government

[68]The Economist Intelligence Unit, 'Democracy Index 2020: In sickness and in health?' (2021) 8–13 <https://bit.ly/3LSbe5I> accessed 1 Dec 2022.

[69]The decline is seen both through V-Dem's Liberal Democracy Index and The Economist's Democracy Index methodologies. See V-DEM, 'V-Dem Liberal democracy Index 2020' (Our World in Data, 2020) <https://bit.ly/3sa74OM> accessed 1 Dec 2022; 'Democracy Index 2020' (n 68) 22–25.

[70]'Internet Freedom Scores' (Freedom House, 2021) <https://bit.ly/3h5Uo5h> accessed 1 Dec 2022.

[71]Steven Feldstein, 'Digital Repression Index 2010-19' (Mendeley Data, 10 Dec 2020) <https://bit.ly/3Y67tQc> accessed 1 Dec 2022.

[72]Between March 2020 and December 2020, 253 initiatives involving the use of technologies collecting some type of personal data were mapped at the national, state and municipal levels in Brazil. These have been developed by a multifaceted network of public and private actors. See Eduardo G Andrade et al, 'Dados Virais: Legado da COVID-19 nas aquisições de tecnologia pelo Poder Público' (Data Privacy BR, 2021) <https://bit.ly/3FyPY47> accessed 1 Dec 2022.

[73]Law No 13,979 (6 Feb 2020) (Brazil) <https://bit.ly/3sa7dli> accessed 1 Dec 2022.

[74]Ministério da Saúde (Ministry of Health), 'Rede Nacional de Dados em Saúde' <https://bit.ly/3v9ruJD> accessed 1 Dec 2022.

https://doi.org/10.1017/asjcl.2022.31 Published online by Cambridge University Press

faced several obstacles to successfully implementing its strategies due to institutional and political challenges.

The first measure was initially set by the Bolsonaro administration in April 2020 in an announced partnership with the five largest telecommunications operators in the country.[75] Through this strategy, the government would have had access to data collected from the cell phones of almost all Brazil's population, which would have then been anonymised and used to identify risky areas through geolocation. Nonetheless, public rebuke and concerns around privacy risks caused President Bolsonaro to retreat from his initial plan and suspend the negotiations with telephone operators.[76] Shortly after the political defeat, the government pushed forward a provisional measure that would have given the country's statistics office access to personal data held by telecommunications companies.[77] However, Bolsonaro's order was met with several challenges in Brazil's Federal Supreme Court, which struck down the measure under the premise that it did not sufficiently explain how the telecommunications databases would be used against COVID-19 nor how the data collected would be protected.[78] The court's concerns with governmental databases were highlighted by the information leakage affecting more than 16 million Brazilian COVID-19 patients in November 2020 and a successful cyberattack against the RNDS in December 2021,which brought the platform offline for a month and caused patients' logs to disappear.[79]

The restrictions on the use of non-consensual data from telecommunications companies constrained other actions by the federal government, but allowed subnational entities (ie, states and municipalities) to develop their own partnerships with private companies, as long as they abided by Brazil's *General Personal Data Protection Law* (*Lei Geral de Proteção de Dados* or LGPD), which sets high standards for data collection and processing – closely resembling the EU's *General Data Protection Regulation* (GDPR).[80] As of December 2021, at least 47 subnational entities in Brazil have done so, and have been using geolocation data collected through public-private partnerships to define their local health policies.[81] One active company in the country has been Google, which partnered with multiple local governments to provide Community Mobility Reports.[82] Another relevant company has been Brazilian In Loco, a local branch of the US-based company Incognia, which provides geolocalisation services to companies and governments.[83]

In addition to the use of geolocation data, the Brazilian government launched a contact-tracing application called *Coronavírus-SUS*, developed by DATASUS, the Informatics Department of Brazil's public-funded healthcare system, the *Sistema Único de Saúde* (SUS).[84] The app's first version was launched in February 2020 with basic features. The second version released in September,

[75]Rafa Santos, 'Uso de dados telefônicos pessoais para combate à Covid-19 gera dúvidas' (Consultor Jurídico, 2 Apr 2020) <https://bit.ly/3s9AbSh> accessed 1 Dec 2022.

[76]Simone Kafruni, 'Bolsonaro veta geolocalização da população por celular' (Correio Braziliense, 13 Apr 2020) <https://bit.ly/3BVNhWV> accessed 1 Dec 2022.

[77]The government alleged that this information would allow the Brazilian Institute of Geography and Statistics (IBGE) to correctly measure the economic and social impacts of COVID-19, which would support public planning. See Provisional Measure No 954 (17 Apr 2020, revoked) (Brazil) <https://bit.ly/3sbUheY> accessed 1 Dec 2022; Ken Silva, 'Covid-19: Brazil's top prosecutor defends telecoms data collection scheme' (Global Data Review, 4 May 2020) <https://bit.ly/3LQp60p> accessed 1 Dec 2022.

[78]Federal Court of Justice (STF), Ação Direta de Inconstitucionalidade No 6,390/DF (7 May 2020) <https://bit.ly/3p7BAah> accessed 1 Dec 2022.

[79]Catalin Cimpanu, 'Personal data of 16 million Brazilian COVID-19 patients exposed online' (ZDNet, 26 Nov 2020) <https://zd.net/3v4jg5I> accessed 1 Dec 2022; TBR Newsroom, 'Hack crashes health systems and Brazil postpones restrictions on travelers' (10 Dec 2021) <https://bit.ly/3FtYIs1> accessed 1 Dec 2022.

[80]See Law No 13,709 (Brazil), art 6 <https://bit.ly/3LWURFk> accessed 1 Dec 2022.

[81]See Andrade et al (n 72) 34–36.

[82]Google, 'COVID-19 Community Mobility Reports' (Feb 2022) <https://bit.ly/3IcEeCZ> accessed 1 Dec 2022.

[83]See Incognia's homepage: Incognia, 'Home Page' <https://www.incognia.com> accessed 1 Dec 2022.

[84]Serviços e Informações do Brasil, 'Coronavírus-SUS' <https://bit.ly/3h7hXhO> accessed 1 Dec 2022.

https://doi.org/10.1017/asjcl.2022.31 Published online by Cambridge University Press

however, implemented the Google/Apple Exposure Notification (GAEN) API,[85] which allowed patients who tested positive to share their results with health authorities and warn other individuals of possible exposures through anonymous, temporary Bluetooth tokens that utilised users' devices for data processing and storage.[86] Nevertheless, the app registered a very low penetration with around 10 million downloads as of November 2020 – less than 5 per cent of Brazil's population.[87]

Besides these two large strategies, local governments also approved pilot projects for the monitoring of citizens via Remotely Piloted Aircraft (or drones)[88] and demand for FRC systems significantly increased in public and private venues, such as airports and schools.[89] The use of these new technologies highlights a growing trend in Brazil as both strategies are being increasingly supported by state agencies and promoted as effective mechanisms to combat crime – a strong argument in a country still faced by high criminality.[90]

While Chinese companies were not behind any of Brazil's pandemic strategies, their technology supported them extensively. Since the late 1990s, Chinese telecommunications companies have gradually gained a greater role in the country, providing hardware and software solutions to local and non-Chinese companies operating in the country. Huawei is a notorious example as the company currently accounts for two local data centres and about 40 percent of wireless communications networks in operation in Brazil.[91] Currently, all national and multinational companies in the sector use its equipment and maintenance services.[92]

Furthermore, Huawei has launched a series of pilot initiatives with local governments promoting the use of smart city projects and FRCs systems in recent years[93] and has also strategically partnered with Brazilian telecommunications giant Oi to commercialise facial recognition technology in the

[85]Apple and Google jointly developed an API that allowed authorised health officials to create Bluetooth-enabled contact tracing applications. See Apple & Google, 'Privacy-Preserving Contact Tracing' <https://apple.co/3FwxssN> accessed 1 Dec 2022.

[86]Jéferson Campos Nobre et al, 'On the Privacy of National Contact Tracing COVID-19 Applications: The Coronavírus-SUS Case' (Anais da XIX Escola Regional de Redes de Computadores, 27 Oct 2021) <https://bit.ly/3uxfQHe> accessed 1 Dec 2022.

[87]ibid 5.

[88]See eg, La Vanguardia, 'Río de Janeiro usa drones con altavoces para dispersar las aglomeraciones durante la pandemia' (Efe, 15 Apr 2020) <https://bit.ly/3h5IhFx> accessed 1 Dec 2022 (showing the use of drones in the city of Rio de Janeiro).

[89]See eg, Flavia Albuquerque, 'Setor de Segurança tem alta de 40% na busca por tecnologia inteligente' (Agência Brasil, 13 Jul 2020) <https://bit.ly/3BHwTsI> accessed 1 Dec 2022 (underscoring that demand for FRCs increased by 12.3% during the first five months of the pandemic); BNAmericas, 'Pandemic accelerates thermal camera sales in LatAm' (21 Apr 2020) <https://bit.ly/3KQmOwY> accessed 1 Dec 2022.

[90]Amanda Lemos, 'Reconhecimento facial cresce no Brasil; vídeo explica como isso afeta você' (Folha de São Paulo, 7 Aug 2021) <https://bit.ly/3Ih9a5a> accessed 1 Dec 2022 (describing how FRCs are becoming a common tool in the toolkit of local policies); Ministério da Justiça e Segurança Pública, 'Portaria n° 793' (24 Oct 2019) <https://bit.ly/33MUtYI> accessed 1 Dec 2022 (federal legislation providing public incentives for the use of facial recognition software to combat crime).

[91]Huawei has been a major technology provider in Brazil for the past 22 years. The country's biggest cellphone operator, Vivo, reportedly uses Huawei's 3G and 4G technology in 65% of its networks. Claro, the second largest operator, acquires 55% of its equipment from Huawei, and Oi, the third largest, 60%. See Felipe Junqueira, 'Operadoras brasileiras pedem transparência e participação da Huawei no 5G' (Canaltech, 29 Nov 2020) <https://bit.ly/3IePsXR> accessed 1 Dec 2022; Maurício Renner, 'Huawei reforça nuvem no Brasil' (Baguete, 29 Jan 2021) <https://bit.ly/35iTRKu> accessed 1 Dec 2022.

[92]Poder 360, 'Portaria permite Huawei no leilão do 5G, mas governo exige rede exclusiva' (29 Jan 2021) <https://bit.ly/3JLw1X0> accessed 1 Dec 2022.

[93]See eg, the partnership between Huawei and Campinas, the 4th largest city in Brazil: Huawei, 'Campinas reforça parceria com a Huawei para implementar soluções de segurança' (14 Dec 2018) <https://bit.ly/3p7SV2C> accessed 1 Dec 2022; and Huawei's partnership with the state of Bahia: Amanda Palma & Clarissa Pacheco, 'Presos pela cara: polêmico sistema de reconhecimento facial identificou 109 foragidos na BA' (Correio, 5 Jan 2020) <https://glo.bo/33GJqjA/> accessed 1 Dec 2022; Finally, see eg, Huawei's Smart Cities promotion event in Curitiba: Redação Digital Security, 'Solução para Smart City da Huawei será destaque na Smart City Expo em Curitiba' (Revista Digital Security, 21 Mar 2019) <https://bit.ly/3Iebie0> accessed 1 Dec 2022.

https://doi.org/10.1017/asjcl.2022.31 Published online by Cambridge University Press

country.[94] Besides Huawei, other companies such as ZTE, Dahua and Hikvision have also become increasingly relevant in the local market.[95] The latter two have been particularly active in providing facial recognition hardware and software to government agencies before and during the pandemic.[96] In 2020, at least 13 new projects were mapped between these companies and public authorities aimed at pandemic control.[97] Their projects included, eg, AI-enabled camera solutions for identifying individuals, measuring temperature and detecting mask use. Although they are not the only ones operating in Brazil's market, their range is impressive and it is estimated that they have already developed about 266,000 camera systems in the country.[98]

Therefore, the role of Chinese companies and their equipment in current discussions on technology regulation in the country is somewhat disputed. On the one hand, there are no obvious causal links that the Chinese government or its companies have influenced, or sought to influence, Brazil's take on data governance or pandemic management. On the other hand, the digital infrastructure deployed by Chinese companies has supplied Brazilian and non-Chinese actors with new digital tools that have strengthened their capacity to collect data on Brazil's population. Moreover, although the adherence to the surveillance solutions of Chinese companies did not attract particular attention from Brazil's public opinion throughout the pandemic, the growing collecting of data from such technologies has propelled discussions about data governance currently taking place in the country, especially regarding the implementation of 5 G networks and the widespread use of FRCs.

In the first case, Huawei has been in the spotlight around the discussions about its participation in Brazil's much anticipated 5 G spectrum auction. Although public officials initially rejected its participation due to concerns on data security – following the US 'Clean Network' proposal[99] – the government backed off and allowed the use of Chinese technology, restricting it from the government's stand-alone private network.[100] Now, the company is expected to be the likely supplier of all major telecommunications operators in the 5 G local market.[101] The change in position was the last chapter of a long struggle between the Bolsonaro's administration and the Chinese government, and had as background the supply of Chinese vaccines to the country.[102] China's biopharmaceutical Sinovac increased its shipments of Active Pharmaceutical Ingredients for the local production of CoronaVac vaccines after Brazil signalled it would not ban Huawei from the 2021 auctions as the country faced vaccine shortages.[103]

[94]Paulo Soprana, 'Chinesa Huawei faz parceria com Oi para câmeras de reconhecimento facial' (Folha de São Paulo, 16 Oct 2018) <https://bit.ly/33Gc04y> accessed 1 Dec 2022.

[95]See eg, Robert Wren Gordon, 'Brazil Assembly Powers Hikvision Local Expansion' (IPVM, 15 Jul 2020) <https://bit.ly/3h4iltR> accessed 1 Dec 2022 (highlighting that Hikvision is the only foreign video surveillance manufacturer with such an operation inside of a Brazil in the Manaus free trade zone).

[96]Carolina Reis et al, 'Vigilância Automatizada: uso de reconhecimento facial pela Administração Pública' (LAPIN, Jul 2021) (finding that most of FRC devices used by Brazil's public sector come from China, although companies from the US, UK and Israel have also been important suppliers to the Brazilian market).

[97]See Andrade et al (n 72) 36–37.

[98]Simon Migliano & Samuel Woodhams, 'Hikvision and Dahua Surveillance Cameras: Global Locations Report' (Top 10 VPN, 3 Dec 2020) <https://bit.ly/33Iyv93> accessed 1 Dec 2022.

[99]Anthony Boadle, 'Brazil backs U.S. Clean Network proposal for transparent 5G technology' (Reuters, 11 Nov 2020) <https://reut.rs/3sZY7H5> accessed 1 Dec 2022.

[100]The legal strategy adopted required a publicly traded shareholding structure for companies taking part in Brazil's stand-alone private network, something Huawei does not meet as a (formally) privately held company. See Rui Maciel, 'A Huawei não quis participar da rede privada do governo? Não foi bem assim' (Canaltech, 13 May 2021) <https://bit.ly/3hapYyK> accessed 1 Dec 2022.

[101]Juan Pedro Tomás, 'Huawei negotiating with most Brazilian telcos for 5G equipment: Report' (RCR Wireless, 22 Nov 2021) <https://bit.ly/3p9n6Xh> accessed 1 Dec 2022.

[102]Julio Wiziack, 'Governo vai baixar tom contra Huawei no 5G para agilizar importação de insumos de vacina da China' (Folha de São Paulo, 21 Jan 2021) <https://bit.ly/3BLksMv> accessed 1 Dec 2022.

[103]ibid.

https://doi.org/10.1017/asjcl.2022.31 Published online by Cambridge University Press

In the second case, as the use of FRCs quickly advanced in the country pushed, to some extent, by Chinese companies' supply and support, legislative and judicial debates have arisen about whether the surveillance technology complies with Brazil's data protection framework. For instance, in April 2022, São Paulo's Justice Court suspended a public announcement for the installation of FRCs in the city's metro due to concerns on its non-compliance with the LGPD – a dispute Chinese companies were expected to take part in.[104] The issue is now waiting for national legislation on the topic or a decision by the country's independent data authority. São Paulo's example is just one in a series of other embroiled discussions happening in the country as local governments and private companies that have adopted the technology now face legal challenges.[105] In this regulatory vacuum, it has been easy for surveillance companies, including Chinese, to move into Brazil.

It is important to highlight that Chinese companies are not the only suppliers of these technologies;[106] nevertheless, their pilot projects and public-private partnerships have played a remarkable role in promoting their products locally. Brazil's case illustrates how the presence of Chinese companies can supply surveillance tools when local demand calls for it, but their implementation is ultimately constrained by local conditionalities.

South Africa

The widespread use of digital technologies was also a critical feature in addressing the COVID-19 crisis in South Africa. Most prominent digital strategies included applications dedicated to contact tracing via Bluetooth technologies and CCTV networks. Accordingly, discussions about the potential abuse of digital technology have also been particularly salient given the personalised nature of data being processed and captured. Furthermore, South Africa has received telecommunications financing and infrastructure from China in recent years and is one of the top destinations for Chinese ICT companies in Africa.[107] Huawei and ZTE have established their regional head-quarters and logistics centre in the country,[108] and Huawei has partnered with local companies such as South Africa's MTN, Africa's largest mobile operator, to expand the country's network infrastructure in the face of growing local demand.[109] Thus, the digital infrastructure provided by Chinese companies was part of South Africa's pandemic response; however, as in the case of Brazil, it was not directly run by Chinese operators.

When the first cases of COVID-19 were registered in South Africa, President Cyril Ramaphosa swiftly declared a national state of disaster on March 2020, invoking section 27(1)(b) of the *Disaster Management Act 57 of 2002* (DMA) and declaring contact tracing as a necessary strategy to combat the pandemic.[110] The government then passed a series of regulations in the Government Gazette that allowed the identification of infection hotspots using collected data and epidemiological

[104]Interlocutory Appeal no 2079077-58.2022.8.26.0000 Tribunal de Justiça de São Paulo. See Elaine Patricia Cruz, 'TJ mantém proibição de câmeras de reconhecimento facial no Metrô de SP' (Agência Brasil, 18 Apr 2022) <https://bit.ly/3SFqWF0> accessed 1 Dec 2022.

[105]See eg, Victoria Damasceno & Samuel Fernandes, 'Sob críticas, reconhecimento facial chega a 20 Estados do país' (Folha de São Paulo, 9 Jul 2021) <https://bit.ly/352Y2KJ> accessed 1 Dec 2022 (showing that 20 states in Brazil have already adopted FRCs although the LGPD does not provide specific safeguards for this type of technology).

[106]Other relevant providers are, e.g., Admobilize (US), Ineo Infracon (France), Johnson Controls (Ireland) Tecway, Engie and Brisanet (Brazil). See 'Facial recognition in Latin America: Trends in the implementation of a perverse technology' (AlSur, 2021) 11 <https://bit.ly/3qciZKQ> accessed 1 Dec 2022.

[107]Amy Tong, 'China's ICT Engagement in Africa: A Comparative Analysis' (The Yale Review of International Studies, Feb 2021) <http://yris.yira.org/essays/4702> accessed 1 Dec 2022.

[108]Institute of Developing Economies, 'China's Telecommunications Footprint in Africa' (Japan External Trade Organisation, 2021) <https://bit.ly/3vfpKPn> accessed 1 Dec 2022.

[109]ibid.

[110]Frans Viljoen et al, 'Implications of Digital Contact Tracing for COVID-19 in South Africa' (2020) 20 African Human Rights Law Journal 540, 544.

https://doi.org/10.1017/asjcl.2022.31 Published online by Cambridge University Press

maps,[111] wherein the use of smartphone apps for automated contact tracing was considered one of the most promising advances in the fight against COVID-19, as smartphones are ubiquitous in South Africa.[112] To this end, the South African government introduced two mobile voluntary applications and one WhatsApp-based symptom reporting process designed to assist health officials in tracking down exposures after infected individuals have been identified.[113] These strategies were developed by government agencies in partnership with the local private sector; nevertheless, they used digital infrastructure deployed by Chinese companies in the country, especially mobile networks.

The first application (COVID Alert SA) was launched in September 2020 and uses a phone's Bluetooth signal to share a unique code, which is sent to other users of the application within a two-meter radius.[114] The app was developed by the local company Discovery Limited in partnership with South Africa's National Department of Health. People who have tested positive for COVID-19 within two weeks can anonymously alert others by clicking the notification button on the application. However, the person with COVID-19 has the decision on whether to voluntarily share their status. The purpose of the application is to notify users who have been in contact with someone who has tested positive for COVID-19. Accordingly, it encourages people to isolate and test for COVID-19 as a measure to further prevent infections. The COVID Alert SA application is predicated on smartphone technology which was developed by Apple and Google, specifically the GAEN API.[115]

To deal with privacy risks, including the potential for temporary rights-infringing measures to become permanent features, the COVID Alert application does not record any personal or health information. More exactly, individual phones exchange anonymised digital identities to mark such interactions.[116] Data is stored on individual devices and users can opt out anytime. The unique codes cannot be used to identify a phone number or identity; therefore, data cannot be traced back by technical means to persons, locations or devices. The unique Bluetooth identifier codes change every ten to twenty minutes, to help prevent tracking. This mechanism provides the user with full authority and control over who gets access to the data, which has been coined as 'Self-Sovereign Identity'.[117]

The second application (Covi-ID) was developed in a partnership between government agencies and the University of Cape Town.[118] The application uses a similar technology of COVID Alerta SA, collecting an infected subject's geolocation and sharing it through Bluetooth anonymised tokens when authorised.[119] Similarly, the personal information is saved on the data subject's personal device and not on a centralised government database.[120] The application also allows users to present QR codes and for verifiers to scan these QR codes to retrieve the user's COVID-19 health status – a

[111]'Regulations and Guidelines – Coronavirus Covid-19' (South African Government, 2021) <https://bit.ly/3JDqdyG> accessed 1 Dec 2022.

[112]South Africa is one of the largest mobile markets in Africa. Nine in ten adult South Africans have a mobile device and around 51 per cent of cell phone owners have a smartphone that can access the internet and apps. See Laura Silver & Courtney Johnson, 'Majorities in Sub-Saharan Africa own mobile phones, but smartphone adoption is modest' (Pew Research Center, Oct 2018) <https://pewrsr.ch/3BFf5P3> accessed 1 Dec 2022.

[113]'COVID-19 Online Resource and News Portal' (Health Department of South Africa, 2021) <https://bit.ly/3LP4upv> accessed 1 Dec 2022.

[114]'Apps: South Africa Project Report' (Alt Advisory, 2020) <https://bit.ly/3JPyQ9A> accessed 1 Dec 2022.

[115]ibid.

[116]Jonathan Klaaren et al, 'South Africa's COVID-19 Tracing Database: Risks and rewards of which doctors should be aware' (2020) 110 SAMJ: South African Medical Journal 617, 617–620 <https://bit.ly/3JNZfUY> accessed 1 Dec 2022.

[117]Marco Schepers & Zinhle Novazi, 'COVI-ID: SA's contact tracing app ensures protection of privacy' (Tabacks, 3 Jun 2020) <https://bit.ly/3iN5Abi> accessed 1 Dec 2022.

[118]Google Play, 'Covi-ID' <https://play.google.com/store/apps/details?hl=en&id=com.coviid> accessed 1 Dec 2022.

[119]See Schepers & Novazi (n 117).

[120]ibid.

https://doi.org/10.1017/asjcl.2022.31 Published online by Cambridge University Press

tool closely resembling China's Alipay Health Code. The Covi-ID app makes use of a GDPR based privacy policy and is said to comply with the *Protection of Personal Information Act 4 of 2013* (POPIA), South Africa's benchmark for data protection, which came into force in July 2020.[121] Nevertheless, the app registered a remarkably small number of downloads as it was not rolled out extensively by the government.[122]

Finally, the WhatsApp symptom tracker (COVIDConnect) was developed by diverse South African public and private actors, including Telkom, Praekelt, GovChat, and the Council for Scientific and Industrial Research. It was launched nationwide in May 2020 by South Africa's Department of Health.[123] The platform uses machine learning technology to deliver automated responses with information on COVID-19 including symptoms recommendations, travel advice, and the latest country data. The platform was hailed as an effective strategy to diffuse reliable information on the pandemic; however, it is unclear who has been processing the information submitted and where else it may be disclosed since there are no terms and conditions available regarding the use of this functionality. After having been successful in South Africa reaching over 2.6 million users, a similar platform was adopted by the World Health Organisation (WHO) inspired by the South African strategy.[124]

Before the introduction of these three tools, the South African government utilised a tracing database, which collected both aggregated and individualised mobility and locational data on COVID-19 cases and their contacts from telecommunications service providers.[125] The database was licensed under the *Electronic Communications Act 36 of 2005* and recorded, under the written request of the Director-General of Health, the names, identities, and cellphone numbers of people who tested for COVID-19.[126] Although there were compelling public health reasons for this development, it allegedly infringed on constitutional privacy rights and the POPIA as South Africans were vulnerable to non-consensual processing of their personal information.[127] Against this background, the South African Government implemented a set of track-and-trace regulations, in terms of section 27(2) of the DMA.[128] The regulations set out the standards for processing personal information used in the management and containment of the spread of COVID-19. They allow the obtaining of information by the government in relation to location data of any person from electronic communications service providers while establishing legal constraints. In doing so, the government gave effect to the constitutional right to privacy and to prevention mechanisms of the POPIA that had yet to come into effect.[129]

Even with the privacy-preserving protocols taken by the government, data collection processes and security were seen to lack transparency. The South African government contended that to protect data against unauthorised access and usage, its tools make use of a variety of technical security

[121]South African Government, 'Personal Information Act 4 of 2013' (26 Nov 2013) <https://bit.ly/36nIyBm> accessed 1 Dec 2022.

[122]'Tracking the Global Response to COVID-19' (Privacy International, 2022) <https://bit.ly/36rNOnz> accessed 1 Dec 2022; see Alt Advisory (n 114) 13.

[123]Farei Shawn Matiashe, 'WHO adopts Whatsapp platform developed in South Africa to provide information on the coronavirus outbreak' (Business & Human Rights Resource Centre, 27 Mar 2020) <https://bit.ly/35ir8FY> accessed 1 Dec 2022.

[124]WhatsApp, 'The World Health Organization launches WHO Health Alert on WhatsApp' <https://www.whatsapp.com/coronavirus/who> accessed 1 Dec 2022.

[125]Philip de Wet, 'South Africa will be tracking cellphones to fight the Covid-19 virus' (Business Insider, 25 Mar 2020) <https://bit.ly/3IfwrnZ> accessed 1 Dec 2022.

[126]Ignatius M Viljoen et al, 'Contact tracing during the COVID-19 pandemic: Protection of personal information in South Africa' (2020) 13 South African Journal of Bioethics and Law 20.

[127]Specifically, South African Constitution, s 7(2). See South African Government, 'Constitution of the Republic of South Africa, 1996' <https://bit.ly/3JLxwV8> accessed 1 Dec 2022.

[128]All regulations, directions and guidelines relating to COVID-19 in South Africa can be accessed at: South African Government (n 111).

[129]Marco Schepers, Zinhle Novazi & Andrew Attieh, 'Pandemic control through the use of Personal Data' (Tabacks, 4 May 2020) <https://bit.ly/3IbKET6> accessed 1 Dec 2022.

https://doi.org/10.1017/asjcl.2022.31 Published online by Cambridge University Press

measures, which includes encryption, pseudonymisation, logging access controls and restrictions.[130] For instance, the South African National Department of Health and its partners such as Discovery Limited and Telkom supposedly employ confidentiality agreements to combat data leakages. However, how exactly this data is being transmitted and managed by contractors remains unclear. Moreover, despite these procedures, there was a spike in cyberattacks during the COVID-19 pandemic against government agencies, which increased the public's awareness of data breaches.[131]

Finally, South Africa's response to COVID also included the use of digital CCTV networks. These closed-circuit surveillance tools were periodically utilised by the police during countrywide lockdowns that included bans on gatherings, a curfew from 9pm to 4am and prohibition on the sale of alcohol.[132] This was a containment strategy that aimed at limiting social interaction while supposedly preserving the economy. Technology procured from Chinese companies provided the infrastructure that underpins this digital surveillance practice, which is, in part, linked with Huawei's Safe Cities projects in the country.[133] These initiatives utilise a plethora of interconnected systems like video cameras, tracking devices, software, and cloud storage systems to tap public and private platforms in a more cohesive manner to advance service delivery and policing.[134] Besides Huawei, Vumacam, a local company, is also a leading provider of networked surveillance cameras.[135] For example, Johannesburg's central business district is contingent on digital CCTV cameras procured from Huawei and Vumacam, but also from Axiom, a South African digital surveillance camera provider, Iveda, an American supplier, and Hikvision, a Chinese state-owned supplier.[136] The City's extensive camera surveillance system is located within the Integrated Intelligence Operations Center and these various cameras are owned by the police, local municipalities, and private security companies.[137] By purchasing governance and monitoring tools through various commercial channels, South African state and private actors are able to establish a hybridised surveillance system that is part of a broader digital infrastructure initiative.[138]

South Africa illustrates, like Brazil, that Chinese companies have been key in providing the digital infrastructure needed for the contact tracing strategies implemented throughout the pandemic, even though they were operated and designed by partnerships between local public and private actors. Moreover, South Africa's smart cities show how often these infrastructure networks, which rely on Western and Chinese corporations, highlight host nations' aptitude to patch together diversely sourced technology.

Vietnam

Vietnam has been commended for having a successful response to the COVID-19 pandemic, particularly prior to the arrival of the Delta variant.[139] Building on institutional capacity and prior

[130]Health Department of South Africa, 'COVID-19 Online Resource and News Portal' https://bit.ly/3LP4upv accessed 1 Dec 2022.

[131]See eg, TimesLive, 'Massive data attack exposes personal info of 24 million South Africans' (Sunday Times, 19 Aug 2020) <https://bit.ly/3halW9Q> accessed 1 Dec 2022.

[132]Alexander Winning, 'South Africa extends tight COVID-19 restrictions for another 14 days.' (Reuters, 12 Jul 2021) <https://reut.rs/3JPRZYD> accessed 1 Dec 2022.

[133]Feldstein, 'Hearing on China's Strategic Aims in Africa' (n 33).

[134]'Huawei Smart City Overview Presentation' (Huawei, Jun 2018) <https://bit.ly/3Hp9UEh> accessed 1 Dec 2022.

[135]Karen Allen & Isel van Zyl, 'Who's watching who?' (ENACT, Issue 11, Nov 2020) <https://bit.ly/3IfdVfs> accessed 1 Dec 2022.

[136]Chris Burt, 'Iveda brings biometrics and surveillance analytics to South Africa with AXIOM partnership' (Biometric Update.com, 7 Jun 2019) <https://bit.ly/35iqxnI> accessed 1 Dec 2022.

[137]Dorcus Basimanyane & Dumisani Gandhi, 'Striking a balance between CCTV surveillance and the digital right to privacy in South Africa' (APCOF, 27 Dec 2019) <https://bit.ly/3sYIdN5> accessed 1 Dec 2022.

[138]'IIOC provides for intelligent policing using CCTV cameras' (Media release, City of Johannesburg, 2018) <https://bit.ly/3HbsKhO> accessed 1 Dec 2022.

[139]Emma Willoughby, 'An ideal public health model? Vietnam's state-led, preventative, low-cost response to COVID-19' (Brookings, 29 Jun 2021) <https://brook.gs/3LPBwWm> accessed 1 Dec 2022.

https://doi.org/10.1017/asjcl.2022.31 Published online by Cambridge University Press

experiences with SARS, the government prioritised contact tracing and targeted quarantines while using data surveillance and mobile application infrastructure to manage the pandemic. Similar to China's response, Vietnam's response also relied on local government coordination and surveillance technology building on infrastructure developed with domestic Vietnamese technology companies. However, Vietnam's experience is noteworthy for its distinction from the other two case studies: that despite Vietnam officially rejecting economic entanglement with Chinese technology firms, it has also increased its domestic digital surveillance both before and during the COVID-19 pandemic through active exposure to Chinese models of surveillance, including technical training from Chinese authorities and companies.[140] Thus, Vietnam's experience illustrates that the practices of the Chinese government, even if not directly adopted into a country through partnerships with Chinese technology companies, may cause a diffuse effect in providing replicable strategies favourable to authoritarian governments. It can offer, for instance, a cover that normalises the adoption of more authoritarian surveillance practices, such as those that Vietnam seeks to pursue with its own companies as a model of both economic development and political control.[141]

Building on its prior experience with other contagious diseases, such as the SARS pandemic, Vietnam has over time prepared and invested in a series of measures for public health emergencies, including its national public health surveillance system.[142] In 2009, Vietnam first employed a nearly real-time and web-based system to collect and aggregate public data and, since 2016, hospitals have been required to report notifiable diseases within 24 hours to a centralised database.[143] Vietnam has also looked to Western support to develop pandemic responsiveness and even surveillance strategies, in particular for illnesses that may spread across its borders. In 2018, in collaboration with the US Centers for Disease Control and Prevention (CDC), Vietnam implemented an 'event-based' surveillance program.[144] The program is designed to enable members of the public, including teachers, pharmacists, religious leaders, and even traditional medicine healers, to report public health events. All these strategies were part of the country's COVID-19 pandemic response and are part of the country's national strategy to implement a smart healthcare industry that encompasses disease prevention, medical examinations, and health management through a digital health ecosystem.[145]

When COVID-19 arrived in Vietnam, surveillance and contact tracing were central to the country's strategy. After the first cases were registered, Prime Minister Nguyễn Xuân Phúc established a ministerial task force to design and implement a national response that was set to include the use of digital infrastructure.[146] The head of Vietnam's official Steering Committee for COVID-19 Prevention and Control tasked the Ministry of Health (MOH) and the Ministry of Information

[140]See eg, Shahbaz (n 25) 2–10; Justin Sherman, 'Vietnam's Internet Control: Following in China's Footsteps?' (The Diplomat, 11 Dec 2019) <https://bit.ly/3HaBy7x> accessed 1 Dec 2022 (arguing that China's exports to Vietnam have encouraged the adoption of authoritarian internet control practices); Trinh Huu Long, 'Vietnam's Cybersecurity Draft Law: Made in China?' (The Vietnamese, 8 Nov 2017) <https://bit.ly/3JIKdjt> accessed 1 Dec 2022; He Huifeng, 'In a remote corner of China, Beijing is trying to export its model by training foreign officials the Chinese way' (South China Morning Post, 14 Jul 2018); 'How China is supplying surveillance technology and training around the world' (Privacy International, Feb 2019).

[141]Scholars have already observed diffuse regulatory effects that China's engagement produces in Vietnam through other economic sectors. See Matthew Erie & Do Hai Ha, 'Law and Development Minus Legal Transplants: The Example of China in Vietnam' (2021) 8 Asian Journal of Law and Society 372.

[142]'Viet Nam SARS-free' (World Health Organisation, 28 Apr 2003) <https://bit.ly/3Ie7WHU> accessed 1 Dec 2022.

[143]KPMG & Oxford University Clinical Research Unit, 'Digital Health in Vietnam: Market Intelligence Report' (Dec 2020) <https://bit.ly/3LN1PfX> accessed 1 Dec 2022.

[144]US Centers for Disease Control and Prevention, 'Vietnam update: community-based surveillance yields results' (2017) 25 Updates from the Field <https://bit.ly/3va5kHf> accessed 1 Dec 2022.

[145]See KPMG & Oxford University Clinical Research Unit (n 143).

[146]Thi Phuong Thao Tran et al, 'Rapid response to the COVID-19 pandemic: Vietnam government's experience and preliminary success' (2020) 10 Journal of Global Health 020502 <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7567433/> accessed 1 Dec 2022.

https://doi.org/10.1017/asjcl.2022.31 Published online by Cambridge University Press

and Communications to create surveillance, contact tracing and information dissemination applications within a week of the first COVID-19 cases in Vietnam.[147] To monitor citizens' movement, Vietnam then mobilised digital health applications, building on its robust information and technology sector and high mobile penetration.[148]

Vietnam's contact tracing was comprehensive, as three degrees of contacts were traced for each positive case. To effectively track each case, local public health officials, with support from the military and civil servants, worked with patients to identify who they might have been in contact with in the past 14 days. If any individual tested positive, they were placed in government-run quarantine centres put in place to reduce household and community transmission. Similar to China, Vietnam was noted to have benefitted from its centralised authoritarian political structure, although many levels of government support and buy-in were necessary to facilitate the response, including at the local level.[149]

Vietnam's surveillance efforts also relied on three smartphone apps, which have been voluntary to download: (i) NCOVI, an official state platform for state agencies to distribute rapid updates and public health recommendations; (ii) SmartCity, an application that infected and quarantined people must also download and which notifies the heads of households if a person travels 30 metres from their quarantine area; and (iii) Bluezone, another application launched by the MOH which leverages Bluetooth Low Energy to alert users if they were in close contact with someone who tested positive for COVID-19.[150] The Vietnam government also developed a community monitoring system using GPS technology in Hanoi through the city's Smart City project.[151] Later, the government launched a unified mobile app for COVID-19 prevention, the PC-Covid Vietnam app, which combined existing features of the applications into one travel and social pass – a similar strategy to China's pandemic management.[152] Developed by Viettel Group, Vietnam's COVID-19 immunisation management platform was launched in October 2021 to aid the government's mass vaccination drive and comprised four systems including an e-health record app, a COVID-19 vaccination information portal, a national vaccination support system and a response centre, while also handling registrations for COVID-19 immunisation and tracking vaccination records.

Although Vietnam initially may seem a natural match for Chinese companies given existing close economic ties with China as well as ideological and political sympathies, it is notable that the country has sought to distance its pandemic response from Chinese digital infrastructure due to Vietnam's scepticism of Chinese technology dominance. In recent years, Vietnam has shied away from embracing Chinese companies due to geopolitical concerns,[153] including intentionally rejecting Chinese 5 G technology – a distinct move compared to other countries in Southeast Asia that are openly deploying such technology through Huawei.[154] The country has instead mimicked China and South Korea's development approach by endorsing home-grown companies for economic development. Viettel Group, Vietnam's largest mobile carrier state-owned by the Defense

[147]'NCOVI and Bluezone in Vietnam: Government Launches Digital Apps to Contain COVID-19' (Exemplars in Global Health, 2021) <https://bit.ly/3p8r8iL> accessed 1 Dec 2022.

[148]Smartphones are the most popular device in Vietnam with 93% penetration and more than half of the population (53%) have mobile connection via broadband (3G–5G) with high speed. See 'Mobile Landscape in Vietnam 2019-2020' (MMA, Dec 2020) <https://bit.ly/350BPNx> accessed 1 Dec 2022.

[149]World Health Organisation Representation Office for Viet Nam, 'Viet Nam COVID-19 Situation Report #1' (19 Jul 2020) <https://bit.ly/3BKnXmE> accessed 1 Dec 2022.

[150]ibid.

[151]Nổi Bật, 'Ứng dụng SmartCity hỗ trợ cơ quan chức năng Hà Nội giám sát người cách ly' (Cần Biết, 20 Mar 2020) <https://bit.ly/3Hefwkt> accessed 1 Dec 2022.

[152]Adam Ang, 'Vietnam launches unified mobile app for COVID-19 prevention and control' (HIMSS, 5 Oct 2021) <https://bit.ly/3H5sjWo> accessed 1 Dec 2022.

[153]Raymond Zhong, 'Is Huawei a Security Threat? Vietnam Isn't Taking Any Chances' (The New York Times, 18 Jul 2019) <https://nyti.ms/34V46VR> accessed 1 Dec 2022.

[154]ibid.

https://doi.org/10.1017/asjcl.2022.31 Published online by Cambridge University Press

Ministry, announced their own successful 5 G development while already using Ericsson's and Nokia's technology for its 4 G network.[155] Other smaller carriers, such as MobiFone Corp and Vinaphone, have followed the same path rejecting Chinese companies' hardware as well.[156]

Shying away from Chinese companies, Vietnam has also invested in artificial intelligence and facial recognition applications developed by its domestic industry.[157] Nevertheless, it is important to note that its general surveillance system has increased over the years, with similarities and training received from the Chinese regime, as well as some technological infrastructure to support this expansion.[158] For instance, companies such as Hikvision and Dahua still have a strong foothold in Vietnam as the country registers more than 822,000 camera networks from these companies combined – both companies' largest market in the world.[159]

Against this background, Vietnam's surveillance and quarantine approaches both in handling the COVID-19 pandemic and in creating state surveillance outside of the pandemic have been similar to China's, involving the mobilisation of mobile technology penetration, surveillance applications, local actors' coordination, and targeted quarantines. However, Vietnam serves as an interesting case study in which Chinese influence may have informed its general surveillance approach, while the specific use of Chinese technology has been rejected. Simultaneously, Vietnam adapted its own surveillance program, which was strongly aided by the centralisation of its authoritarian government structure and built on its prior experiences with the SARS and Middle East respiratory syndrome pandemics, in collaboration with foreign actors such as the US CDC. Therefore, Vietnam is notable as an authoritarian regime that has successfully embraced digital surveillance as a pandemic response, despite simultaneously rejecting the direct use of Chinese technology and companies.

Reflections on Chinese Influence in Pandemic-Related Digital Surveillance Trends

While a sample of three countries is a small one, it is nevertheless representative of certain trends on how Chinese digital infrastructure has been deployed and adapted in foreign jurisdictions during the pandemic. The use of digital surveillance technology in managing the pandemic also provides insight as to how scholars and observers might reconceptualise issues related to the global spread of surveillance practices and, more specifically, to China's influence in domestic technology governance abroad. Our focus on Chinese technology does not suggest China's exceptional nature in the distribution of surveillance goods or seeks to obscure the broader transnational market of digital surveillance tools, which includes several other international actors. However, our narrow approach may be warranted if it elucidates China's opaque role in the development of global ICT markets and in the general spread of digital surveillance practices.

In this regard, data from our case studies show no evidence to support the claims that the Chinese government and its companies have exploited the pandemic to export digital repression to other jurisdictions, at least when export suggests a deliberate aim to promote surveillance practices. Evidence like this seems unlikely to arise, as proof of such claims would appear to rely on

[155]Tomoya Onishi, Vietnam's top telecom to adopt "self-developed" 5G tech' (Nikkei, 10 Apr 2019) <https://s.nikkei.com/3BJL00L> accessed 1 Dec 2022.

[156]John Boudreau & Nguyen Dieu Tu Uyen, 'Vietnam prefers its mobile networks to be free of Huawei' (The Jakarta Post, 26 Aug 2019) <https://bit.ly/36rxWBr> accessed 1 Dec 2022 (explaining that the Philippines, Thailand and Malaysia have showed openness to deploy Huawei's technology).

[157]'Vietnam engineers develop state-of-the-art face recognition technology' (Viet Nam News/Asia News Network, 21 Apr 2020) <https://bit.ly/35lYF21> accessed 1 Dec 2022.

[158]Trien Vinh Le, 'Will Vietnam Follow China's Model for Digital Dictatorship?' (The Diplomat, 22 Jun 2019) <https://bit.ly/3BHquxA> accessed 1 Dec 2022.

[159]See Migliano & Woodhams (n 98).

https://doi.org/10.1017/asjcl.2022.31 Published online by Cambridge University Press

internal accounts whistle-blowing the situation or policy statements focused on such goals, which have not surfaced in relation to China's digital strategy during the pandemic.[160] This conclusion also seems to overshadow the fact that China's own pandemic-related surveillance resulted from a particular environment that is not easily replicated by partner countries.

There may be a better argument, nevertheless, under a weaker interpretation of export, wherein the claim is that Chinese surveillance technology alone is leading to different governance outcomes than those originating from liberal democracies. As seen in our study, the pandemic highlighted that surveillance models are spreading across the world, made possible, to some extent, by the technical support offered by Chinese companies or the influence of the Chinese government as a role model. However, the meeting point between Chinese surveillance technology and host nations' demand has not had the same characteristics as what it looks like in China, as local stakeholders also dictate outcomes of the development of ICT infrastructure and surveillance practices.

Thus, having in mind that Chinese technology and governance models have either supported or influenced our country sample's pandemic management strategies, our examination of the evidence shows different fashions in which host countries are adapting Chinese technology for their own needs. Precisely, we observe three general trends of Chinese influence proliferating diffusely in our sample of countries: (i) Chinese technology supported or influenced the management of the pandemic; however, each country designed and operationalised its response framed on its own technical and institutional capacities; (ii) the use of Chinese technology or governance models within each country's pandemic response blended with those from domestic or non-Chinese foreign companies; and (iii) countries acquired implementation capacity to develop surveillance strategies through technical exchanges with Chinese actors (ie, companies and government agencies) without necessarily adhering to Chinese technology.

First, we observe that the export of Chinese technology is increasingly providing governments with digital infrastructure that may be used for surveillance purposes, even though countries have not necessarily emulated China's surveillance approach. For instance, our Brazil and South Africa case studies show countries where massive data collection has happened through varied data streams, such as telecommunications networks, which despite being extensively deployed by Chinese companies in both countries, are not usually associated with China's surveillance toolkit. Additionally, the extent to which governments employed such digital infrastructure for surveillance goals seems to have been ostensibly constrained by local contingencies such as legal safeguards and technical capacity. This is particularly the case of Brazil, which experienced a demand increase for facial recognition software throughout the pandemic – enabled in part by Chinese offer and promotion of its surveillance solutions. However, the deployment of such technology has been limited by discussions of its legality under the country's data privacy regime, which is heavily inspired by the EU's GDPR. Thus, we observe that China's supply-side might have influenced data governance abroad during the pandemic by making new digital infrastructure available to a part of our case studies.[161] Yet any supply-side influence seems to have been eventually modulated by demand-side constraints. In other words, Chinese companies have engaged on the terms available in local contexts, which have resulted in contextually contingent outcomes.

Second, we must pay attention to the fact that China has not been the only country contributing to the expansion of global digital surveillance during the pandemic. All three case studies presented

[160]It is important to bear in mind that as more information arrives and the pandemic passes, more analysis will be available to parse through China' growing geopolitical footprint. To this end, other case studies could be useful to disentangle Chinese technology exports from data management influence. For instance, interesting cases are unfolding in Ecuador and Myanmar. See eg, Paul Mozur et al, 'Made in China, Exported to the World: The Surveillance State' (The New York Times, 24 Apr 2019) <https://nyti.ms/3HdDlJ0> accessed 1 Dec 2022; Jason Tower, 'China Using Pandemic Aid to Push Myanmar Economic Corridor' (United States Institute of Peace, 27 May 2020) <https://bit.ly/3LLTYz4> accessed 1 Dec 2022.

[161]See Erie & Streinz (n 14) 42–47 (analysing how Chinese companies providing digital infrastructure to host countries shape the conditions under which these countries transition towards digitally-mediated economies and societies).

https://doi.org/10.1017/asjcl.2022.31 Published online by Cambridge University Press

herein highlight how local and non-Chinese foreign companies also played a role developing and deploying digital surveillance strategies. The widespread use of digital surveillance does not provide a basis on which China's influence during the pandemic can be meaningfully disentangled from that of other countries.[162] Even though Chinese companies have a comparatively larger share of the surveillance technology global market,[163] the pandemic shows that companies from elsewhere in the world seem inclined to step in to offer similar solutions to domestic challenges. In addition, the origin of surveillance technology employed by the observed countries does not seem to have led to a specific approach linked to China's digital governance models. This observation does not neglect Chinese influence via other avenues, such as previously mentioned global internet governance and technical standardisation activities,[164] but it can add to the debate on whether the source of surveillance technology is a determinant factor in data governance design.

Third, our case studies also suggest that inversely, countries might opt to reject Chinese technology while copying China's surveillance approach and acquiring implementation capacity through the provision of technical assistance and capacity building by Chinese actors. Vietnam, which has officially rejected Chinese technology, seems to have been influenced by Chinese approaches of social control, and may also be copying Chinese models of surveillance to both preserve its political power and facilitate economic development through the endorsement of home-grown technology companies. This contradictory finding underscores how the interests of the host country clearly direct the relationship with China and suggests that local factors affect the uptake of Chinese influence. Therefore, the surveillance practices of the Chinese government and companies, even if not directly adopted into a country through economic importation of Chinese technology, may generate a diffuse effect in providing replicable strategies favourable to authoritarian governments and a precedent that normalises the adoption of surveillance practices – especially if seen as a successful model for both economic development and political control.

The fact that Vietnam is deploying its own surveillance strategy also confirms how the picture of why digital repression is advancing globally is more complex than is often portrayed. In this sense, we observe that surveillance can build on more hostile local environments not necessarily linked to China's influence; a notable example being Brazil. In recent years, the country has experienced an alarming rise in digital repression indicators[165] against the backdrop of rising political persecution by the Bolsonaro government and its supporters. This is highlighted as the government itself has pushed forward surveillance programs to monitor the activities of opposing public servants and journalists.[166] The troubled scenario is markedly a consequence of domestically contingent vectors, even though Brazil has been associated with narratives that link growing digital repression to Chinese companies' local surveillance footprint.[167]

As stated before, this paper aims to add a level of complexity to the narrative of China's ambition to export a normative model of digital surveillance and governance. Ultimately, we do not argue that Chinese surveillance technology exports are exempt from having adverse influence on other countries as certain kinds of technologies can encourage the adoption of authoritarian practices. As argued by Duncan, digital surveillance tools, like facial recognition technologies, are not simply

[162]Surveillance practices were also part of many liberal democracies' pandemic responses. See Woodhams (n 4).

[163]See Feldstein, 'The Global Expansion of AI Surveillance' (n 17); ASPI (n 24).

[164]See La Bruyère et al (n 11).

[165]See Feldstein, 'Digital Repression Index 2010-19' (n 71).

[166]Rubens Valente, 'Ação sigilosa do governo mira professores e policiais antifascistas' (UOL, 24 Jul 2020) <https://bit.ly/3vNQXbh> accessed 1 Dec 2022; 'Governo Bolsonaro contrata empresa para espionar jornalistas e personalidades; confira a lista' (RD1, 2 Dec 2020) <https://bit.ly/3s97Lbi> accessed 1 Dec 2022.

[167]See eg, Maria Laura Canineu, 'High-tech surveillance: from China to Brazil?' (Human Rights Watch, 31 May 2019) <https://bit.ly/378ucFj> accessed 1 Dec 2022; Ana Ionova, 'Brazil takes a page from China, taps facial recognition to solve crime' (The Christian Science Monitor, 11 Feb 2020) <https://bit.ly/3MCbu9B> accessed 1 Dec 2022.

https://doi.org/10.1017/asjcl.2022.31 Published online by Cambridge University Press

neutral instruments of governance.[168] Rather, they are political tools that are embedded in a given society and may have negative consequences for the public. These technologies have the capacity to exacerbate established problems at the intersections of inequality, race, gender, and policing. Nevertheless, it is clear that their supply factors must be evaluated alongside demand side conditionalities, in particular legal and political structures. In our case studies, Chinese technology and capital have not been the fundamental drivers of growing digital surveillance during the pandemic, but they can be seen as another factor that supports and exacerbates existing trends such as rising authoritarianism.

In this regard, while host nations' legislation may offer a set of broad principles and commitments, there are still significant gaps in how emerging technologies are regulated in the world. It is this gap between Chinese technology supply and regulatory vacuums that seems to augur the atrophy of democratic norms and civil liberties. In South Africa, for instance, there is no mention of a CCTV code of practice in any legislation, including the POPI Act. Accordingly, there are no robust checks and balances as to how facial recognition software or biometric databases should be managed in Brazil or Vietnam. Thus, regulation of digital surveillance technologies is missing potentially as a mediating factor in Brazil, South Africa, Vietnam and beyond.[169]

Finally, we should also be attentive to how other international actors will react to the growing involvement of Chinese surveillance companies in foreign markets. Most recently, the Biden administration launched an initiative at the Summit for Democracy to curb the exports of technology with surveillance capabilities to countries with poor human rights records.[170] The 'Export Controls and Human Rights Initiative' was signed by the US, Canada, France, the Netherlands, and the United Kingdom, and is set to stem the tide of authoritarian government misuse of technology by establishing a nonbinding written code of conduct on the use of surveillance technology. It is still unclear what role and impact this initiative will have on the exports of these countries and China's companies, especially to developing nations. Companies like Huawei have already stated that they would take effective measures to prevent abuse from using their technology – although their claims remain unclear in practice.[171]

Conclusion

While the expansion of digital surveillance and discussion about its implications pre-dates the pandemic, COVID-19 exacerbated a global trend towards spreading digital surveillance practices. Commentators who saw China as an exporter not just of surveillance technology, but also of the governance of that technology, advanced a theory that China would use the pandemic to spread its technology governance model. To test these claims, this paper has sought to shed light on how national governments deployed digital technologies to curb the COVID-19 virus and whether, if at all, Chinese technologies and companies played a role in domestic management policies and governance.

Through our case studies, we have observed that selected countries were able to implement large-scale surveillance systems due to Chinese and non-Chinese technology already deployed in

[168]Jane Duncan, *Stopping the spies: constructing and resisting the surveillance state in South Africa* (Wits University Press 2018)

[169]In Africa alone, half of the countries still do not have laws on data protection, and, if legislation is in place, it generally does not have clear enforcement mechanisms and strategies for digital surveillance systems. See Brian Daigle, 'Data Protection Laws in Africa: A Pan-African Survey and Noted Trends' (Journal of International Commerce and Economics, Feb 2021) <https://bit.ly/3FxpP5q> accessed 1 Dec 2022.

[170]The White House, 'Fact Sheet: Export Controls and Human Rights Initiative Launched at the Summit for Democracy' (10 Dec 2021) <https://bit.ly/3v6JjsY> accessed 1 Dec 2022.

[171]John Suffolk, 'Cyber Security Perspectives' (Huawei, Oct 2013) <https://bit.ly/33IkU1F> accessed 1 Dec 2022; Jane Zhang, 'Tencent, Huawei, other major Shenzhen firms to bolster user data safeguards ahead of roll-out of new personal information law' (South China Morning Post, 23 Oct 2021) <https://bit.ly/3JMg9Dr> accessed 1 Dec 2022.

https://doi.org/10.1017/asjcl.2022.31 Published online by Cambridge University Press

each country – and did so on their own terms and contingencies. Thus, expansive use of digital surveillance in managing the pandemic appears to have neither been a direct consequence of Chinese technology exports nor its surveillance approaches. Rather, factors such as state capacity to conduct digital surveillance, itself dependent on the existence of digital networks and technical knowledge, as well as political will to use data and make governance changes better explain how countries ultimately used digital surveillance as part of their pandemic response. Similarly, the existence of safeguards intended to balance the need to manage the pandemic and the use of digital surveillance against privacy rights of a state's population appear primarily to have been dependent on the pre-pandemic state of digital governance rather than susceptibility to Chinese influence. Accordingly, a deeper look at the use of digital surveillance in managing the pandemic suggests that the theory of China exporting digital repression, even in some indirect sense, likely oversimplifies reality.

China's intentional desire to export its normative values abroad and its engagement in foreign infrastructure certainly points to supply factors, which foster conditions for the misuse of devices, particularly in political and legal environments that have weak checks and balances. Although individual countries procuring Chinese technology have their own interests, China's active push to support the distribution of surveillance tools also shapes outcomes. Drawing attention to how the party-state leverages demand factors for its own state interests does not necessarily imply downplaying host nations' volition and their ability to detect outcomes; rather, it points to how studies must establish more proportional accounts that are able to examine both the local and global features that determine outcomes.

Most studies highlight the supply factors that motivate the proliferation of Chinese digital surveillance technologies, paying meagre attention to the local factors that determine its use. This paper focuses our attention on the often-neglected minutiae of Chinese operations in local contexts so as to expand our understanding of how China's growing geopolitical footprint is mediated by domestic conditions and actors. This dialectic posture shows how local and global factors are interconnected, deriving illumination and clarity from one another. Crucially, this layered approach hopes to forestall the potential long-term impact of Beijing's growing cyber power on the global stage.

Cite this article: Germanò MA, Liu A, Skebba J, Jili B (2023). Digital Surveillance Trends and Chinese Influence in Light of the COVID-19 Pandemic. *Asian Journal of Comparative Law* **18**, 91–115. https://doi.org/10.1017/asjcl.2022.31