6月
7月
8月
9月
10月
11月
12月
2019年1月
2月
3月
4月
5月
6月
7月
8月
9月
10月

7

SCHEMES, DREAMS, AND NIGHTMARES:

CHINA'S PARADOX(ES) OF TRUST

Gerry Groot

IN EARLY NOVEMBER 2019, the son of Wanda billionaire Wang Jianlin 王健林, Wang Sicong 王思聪, was banned from flying first class, using high-speed trains, and buying luxury goods because he had failed to repay a debt. He was also named and shamed on a publicly accessible Social Credit System 社会信用制度 (SCS) blacklist. He was among some 23 million people who have been similarly punished.[1]

In some places, debtors' faces are flashed on to public television screens when they are in the vicinity or those around them receive phone notifications that a debtor is near. A song, 'Be as Good As Your Word' 说到做到, is just one way the Party-state conveys the Santa-like message: we know if you've been good or bad, so be good for goodness sake.[2] The latest phase in the evolution of these initiatives, embodied in the 2014–2020 Social Credit System plan 国务院关于印发社会信用体系建设规划纲要(2014–2020年)的通知,[3] ends soon, but there is no end in sight to the SCS — just one aspect of what many in the West are calling the People's Republic of China's (PRC) 'surveillance state'.[4] Closed-circuit television (CCTV) cameras are another. Chongqing is now reputed to be 'the world's most surveilled city', with some 2.58 million cameras for a population of fifteen million people.[5] On 1 December 2019, it became mandatory for all applicants for new phone SIM cards across the country to have their faces scanned — supposedly to prevent identity theft, but it also facilitates the use of facial recognition software systems.[6]

In some places, bio-data collection augments video surveillance. An in-depth *New York Times* article about Chinese researchers working on facial imaging based on DNA samples — particularly among the Uyghur Muslim minority of Xinjiang — indicates how bio-data can be integrated into larger systems of surveillance and control.[7] Both Uyghurs and Tibetans are heavily surveilled, policed, and documented right down to recording of their iris patterns, blood types, fingerprinting, and facial scans (see the *China Story Yearbook: Power*, Chapter 4 'Internment and Indoctrination: Xi's "New Era" in Xinjiang', pp.98–111). The Party-state's emphasis on developing artificial intelligence (AI) also feeds into the strengthening of these systems of surveillance and control (see Chapter 5 'AI Dreams and Authoritarian Nightmares', pp.143–154). The new cybersecurity program released on 1 December and based on the *2016 Cybersecurity Law* further strengthens surveillance, censorship, and the control of data in the online sphere. As Steve Dickinson wrote in the *China Law Blog*: 'The core of the plan is for China's Ministry of Security to fully

access the massive amounts of raw data transmitted across Chinese networks and housed on servers in China.'[8] Or, as Guo Qiquan 郭启全, chief engineer in the Cybersecurity Bureau, famously put it: the goal is 'full coverage'. Overseeing it all is the bureau's new director, Wang Yingwei 王瑛玮, who has a PhD in applied mathematics from Peking University and personal experience developing pattern recognition systems for policing purposes.[9]

Big Brother is watching you
Source: Filip Vancoillie, Flickr

Ideology meets technology and surveillance in the app Study Strong China 学习强国, the name of which is also a cognate for 'Study Xi and strengthen the country'. The Party monitors the progress and activity levels of the 100 million–plus users of the app, which is mandatory for party members.[10]

What to Make of All This?

The Netflix drama *Black Mirror* and dystopian analogies conjured up by Western observers potentially misunderstand the nature of China's surveillance state. The present reality, while dark enough, is more complex and fragmented than such totalitarian narratives allow. The use of facial recognition and AI to name and shame jaywalking pedestrians by showing their faces on public screens in the high-tech southern city of Shenzhen, for example, is still only a local initiative. That the AI company involved

wants to link the results to social media accounts such as WeChat,[11] however, is likely a sign of things to come — as are the fast-evolving technologies surrounding and linking bio-data collection and surveillance.

To understand the logic, limitations, and future trajectories of these systems, we should examine the origin and nature of the social credit schemes. One key lies in much older ideas of public shaming, which are evident in the Shenzhen example above, and another in the ancient philosophy of 'legalism': governance by reward and punishment (see Chapter 2 Forum 'Legalism and the Social Credit System', pp.73–77). For these to work as intended, there needs to be a perception of fairness. Anything less than universal implementation of social credit schemes is likely to compound the general lack of public trust in the Party-state at the lower levels, with which the public has the most frequent and direct contact, and if that becomes evident, it can only result in more surveillance and further declines in mutual trust.

China's 'Paradox (es) of Trust'[12]

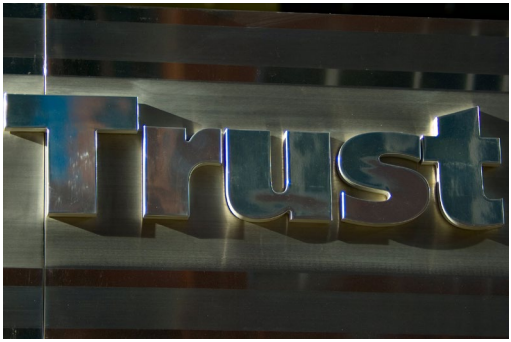
In October, Xi Jinping called for more utilisation of blockchain technology across society to help build a 'trusted system'.[13] Trust 信用 and honesty (sometimes translated as sincerity) 诚信 are social goods that are often in short supply in China. The two are related; as psychologist Nigel Holt has written, 'honesty is a marker that encourages trust and cooperation'.[14] Holt was writing in response to a controversial study conducted in 355 cities across forty countries and published in June 2019 in *Science*. China ranked last in terms of whether people who 'found' a wallet containing the contact information of the 'owner' returned it. Zhou Xinyue 周欣悦 of Zhejiang University was one of many who questioned the survey's methodology, noting that in a separate Chinese study, seventy-one percent of test wallets were neither kept nor returned, but simply left untouched. She notes that behaviour is shaped by 'economic and psychological costs and the culture-specific norm' and that 'active helping and honesty are

distinct concepts'.[15] News reports of the survey stirred both anger and self-searching online, some of which can be found in forums such as *Zhihu* 知乎, which features a category titled 'The honesty crisis 诚信危机'.

The background to this is historical, philosophical, and political. In addition to legalism, China had a strong Confucian tradition that emphasised loyalty within family and clans as well as to the ruler, and a tradition of collective punishment that encouraged self-policing within clans and neighbourhoods. But there was little incentive and no responsibility to look after anyone outside the family, clan, and emperor — and a consequent awareness that strangers similarly had no responsibility to you but were always potentially dangerous — or even ghosts.

After seizing power in 1949, the Chinese Communist Party (CCP) began staging a series of mass political movements that assumed a set percentage of people were 'bad elements' ('rightists', 'counterrevolutionaries', and so on). These movements demanded the participation of ordinary citizens in identifying such people among their peers and colleagues. During the Cultural Revolution (1966–1976), the Party even encouraged children to denounce their parents and teachers. These factors, combined with dramatic reversals of policies and corruption, have all contributed to a trust deficit.

Trust: China ranked last in terms of whether people who found a wallet would return it to its owner
Source: Amy Strachan, Flickr



***Guanxi* builds mutual trust based on the potential for mutual incrimination**
Photo: Neal Sanche, Flickr

For example, personal relations or *guanxi* 关系 make it possible to navigate bureaucracy and business. *Guanxi* is often consolidated by gift-giving (including bribery) and other behaviours, ranging from excessive banqueting to visiting hostess clubs. This builds mutual trust based on the potential for mutual incrimination.[15] Yet such behaviour is itself corrosive of broader social trust because it readily allows people to assume that power and privilege are transactional and not merit based. In addition, at the lower levels, the lack of transparency and procedural fairness as well as exposure to corruption by Party and state officials are generally seen as resulting from the moral failings 失道 or lack of 'quality' 素质 of the officials involved, as opposed to systemic failings of the Party-state system. The National Public Complaints and Proposals Administration 国家信访局 provides a space for venting about problems, yet only a tiny number are ever resolved.[17] When they are resolved, the blame lands on 'immoral' officials and not on structural issues, such as how *guanxi* networks and political imperatives are embedded in administrative systems from top to bottom. As a result, trust in the central levels of the Party and government remains high.[18] The Party-state nonetheless recognises that the issue of trust poses a serious challenge to its legitimacy. So, on the one hand, it pursues highly publicised anticorruption campaigns and, on the other, it builds social credit schemes.

China's Developing Social Credit System(s)

Currently there are some forty rapidly evolving experiments in social credit. China cyber-policy specialist Séverine Arsène likens social credit to a 'chimera' to emphasise its

> patchwork, decentralized and bureaucratic character. Thus far the system is an assemblage of heterogeneous indicators and enforcement mechanisms which differ according to the geographical location individuals find themselves in, and the kind of professional activities they are involved in.[19]

Some systems focus on financial probity. In the twenty-first century, after decades of market reforms and the rise of commercial enterprises in China, banks and other financial institutions need to assess the creditworthiness not only of companies, but also of individuals who may want to take out mortgages or personal loans. With people now freer to move around the country, such data have to be available nationally. Credit China 信用中国, which takes guidance from the People's Bank of China (PBOC), keeps a national public database of blacklisted enterprises and individuals.[20]

As Jeremy Daum of chinalawtranslate.com points out, this system aims to regulate business and force compliance with the law. There are blacklists 黑名单 that lead to punishments, such as that experienced by Wang, and 'red lists' 红名单 that lead to rewards. The designers of local-level systems, guided by central government directions and institutions such as the PBOC, are also adjusting them to protect whistle-blowers who alert authorities to malfeasance and public officials from undue attacks.[21]

These local government social credit systems focus on four key areas: governmental affairs, commercial activity, social behaviour, and encounters with the judicial system. As coordination between government levels, departments, and commercial bodies improves, the goal, according to the State Council, is to

> use credit information exchanges and sharing to bring about linked credit rewards and punishments across multiple departments and regions, making it so that the trustworthy benefit at every turn and the untrustworthy can't move an inch.[22]

For this reason, some observers have described these systems as 'gamifying' social compliance.

Xiamen's Bailu ('egret') score 白鹭分 and Fuzhou's Moli ('jasmine') score 茉莉分 together cover eleven million registered local residents. Local Public Credit Platforms 公共信用信息分享平台 assign scores based on personal data, contributions to the public good (honours, acts benefiting public welfare), financial behaviours (overdue loans, donations to charity, and so on), and legal violations (civil, administrative, and criminal).[23] While most of the negative criteria are objectively measurable, the basis for positive, or red credit is more open to interpretation. Crucially, these schemes are largely voluntary; in 2019, they involved only twenty-one percent of Fuzhou residents and a mere five percent of Xiamen residents. Few low scorers have been penalised; there is at present no legal basis for that. There is neither much public awareness nor much interest in the schemes.[24]

The other layer of complexity in these systems is the role of commercial credit operators, including online payment and credit services and peer-to-peer lending, which has resulted in the wide dispersal of financial data. In 2015, the PBOC allowed a number of companies to trial new credit rating systems; the most famous is Alibaba's Sesame Credit 芝麻信用, which rates users via a points system.[25] But along with companies such as Ant Financial and Tencent Credit, they may also access government blacklists and factor them into their own rankings. It works both ways: some local governments subcontract data management to firms such as Sesame Credit.[26]

As Arsène notes, this has led to a 'wild proliferation of ratings' mixing public and commercial data. She gives the theoretical example of a young

Shanghai resident who might have scores on Sesame, the municipal Honest Shanghai app, and even a third app, Unictown 优你通,[27] which was developed in conjunction with the Communist Youth League Central Committee and the National Development and Reform Commission. The Unictown app is designed 'to give college students and fresh graduates a taste of the rewards brought by having a good social record' and values 'Confucian ethics' such as righteousness, benevolence, good manners, wisdom, and trust.[28] Public information about Unictown offers little clarity about its methodologies.[29] Unictown claims it is designed to reward good behaviour, yet shaming alleged wrongdoers is at least one of its functions.

Surveillance, from Tiananmen to Xinjiang and Beyond

Thirty years after the events of 4 June 1989, the photograph of 'Tank Man' remains an iconic image — at least outside China — about standing up to power.

4 June 1989: 'Tank Man'
Source: Michael Mandiberg, Flickr

On the anniversary of these events, some foreign reporters approached passers-by in Beijing to ask them whether they recognised the image. Police hovered in the background filming the proceedings.[30] Three decades of censorship had been effective: some thought the photo had been taken in another country.

Observing the changes from afar, a Dutch cartoonist drew the Tank Man, but now with his bags full of branded goods, including one from Huawei, transforming him into 'Consumer Man'. Above Consumer Man's head looms a surveillance camera. In 2014, James Areddy described

'Consumer Man'
Source: The Daily Gorilla, Twitter

China's then 100 million surveillance cameras as the legacy of 1989;[31] they are expected to total some 300 million by 2020.

In Xinjiang, cameras are a key element in the system of tracking, control, and intimidation that also uses AI and available databases, so that, for example, police can pull up personal information on a person passing through a checkpoint and know whether they have been to a mosque or, for that matter, a coffee shop that day.[32] According to the tranches of leaked documents published by *The New York Times* and the International Consortium of Investigative Journalists, an additional function of the use of AI is to help the police carry out 'predictive policing'. Since 2016, Xinjiang's Integrated Joint Operations Platform 体化联合作战平台 has been used to pick up 'suspicious actions' and generate lists of those 'who ought to be taken, should be taken' 应收尽收.[33] SenseNets,[34] a Shenzhen-based firm specialising in facial recognition and crowd analysis technology, is working with the Xinjiang government to perfect its surveillance systems.

The current reality across the PRC is of a very messy complex of surveillance systems driven by perceived security concerns, local government needs, higher-level government imperatives, and commercial interests. There is as yet no integrated national system of surveillance, but among the highly advanced surveillance systems being developed are specific technologies such as Yidiantong's 亿点通 Key Person Control database. These target criminals (including parolees, those in community

corrections, and drug users); people seen as threats to social and political stability (petitioners, Uyghurs and other Muslims, rights lawyers, and so on); and others such as members of 'Evil Cults' (see Chapter 2 Forum '"Evil Cults" and Holy Writ', pp.79–82), internal migrants, and the mentally ill. Yidiantong's software also covers those who are considered a threat to national security, extremists, foreigners, and 'online targets' — presumably, critics on social media. Another Yidiantong product, Community Alert 社区警务, maps communities down to the apartment level for the benefit of policing.[35]

Emile Dirks' examinations of tenders led him to conclude that technology suppliers were extending the scope of their databases in response to demands from local public security organs.[36] It is the demand from below rather than orders from above driving much of the mission creep.

Non-Chinese in China are also subject to surveillance, including iris and fingerprint scans at immigration points. TikTok, created by the Chinese company ByteDance, is wildly popular among young people outside China, but when a young American Uyghur woman posted a clip that was ostensibly about makeup but quickly segued to the subject of human rights abuses in Xinjiang, it was deleted, raising concerns about censorship and the potential for such apps to also send user information back to China.[37]

The Carnegie Endowment for International Peace reports that at least seventy-five countries including liberal democracies now use Chinese technology from firms such as Huawei, Hikvision, Dahua, and ZTE, making China the world's largest supplier of surveillance technology.[38] This does not take into account issues raised by Chinese mobile phone technology and apps such as TikTok. The American military is among those concerned by the potential for Chinese actors to remotely access Chinese-made surveillance cameras and systems.[39] Foreign companies, conversely, have been implicated in human rights abuses through sales of surveillance technology to the PRC.

Demands for Better Privacy Protection in China

While censorship ensures that most Chinese are unaware of the literature, movies, and television series that trigger Western fears of totalitarian dystopia, some are pushing back against creeping oversight. Although one survey revealed that sixty to seventy percent of Chinese felt safer because of surveillance, they also expressed concern about the vulnerability of databases and loss of personal information. Increasing numbers of Chinese are becoming sceptical after encountering facial recognition systems — now present in places such as subways and even apartment blocks — that did not work, with negative consequences.[40] In November 2019, one man took a private wildlife park to court for enforcing facial recognition for entry though he had accepted the use of fingerprint scanners in the past.[41] Qinghua professor Lao Dongyan 劳东燕 wrote on WeChat that no attempts had been made to establish any legitimacy for facial recognition on the Beijing subway or even whether it would improve efficiency. Lao also noted that the increasing use of identity checks, even to enter or leave places such as her own university, was hardly a sign of increased trust.[42]

Protestors in Hong Kong — hyper-aware of the consequences of surveillance — have attacked 'smart lampposts' they suspected of being used to monitor them and smashed CCTV cameras in Mass Transit Railway stations and elsewhere. They have famously protected their identities with masks (an 'anti-mask' law was struck down by a Hong Kong court in November, infuriating Beijing), aimed lasers at CCTV cameras during demonstrations, and stuck reflective Mylar on goggles to defeat facial recognition systems.

While general acceptance of social credit and surveillance in mainland China seems to be high, this may change should it become apparent to broader sections of the population that the criminal, deranged, and religious are not its only targets.

Conclusion

China's surveillance systems remain largely fragmented due to the PRC's administrative complexity and wide variations in the ways many different technologies are deployed. It is for reasons such as these that Arsène believes full integration is all but impossible. And yet the systems will continue to multiply. Dirks writes:

Xinjiang's present will become Hong Kong's future
Source: @rhokilpatrick, Twitter

> It is unclear what key individuals these systems will target next. What is clear is that in the absence of robust media or judicial oversight — or any other institutional checks on the Communist Party's domestic security apparatus — key individual management [systems by which individuals are targeted] will continue to metastasize, bringing ever greater swaths of the Chinese public under its control.[43]

The central Party-state under Xi Jinping seeks to increase social trust and hence trust in the government. Yet local experimentation and variations in social surveillance and control not only contribute to the system's incredible complexity. They are also likely to result in unintended consequences and perverse outcomes. Given the opaque interplay between governmental and commercial interests, sooner or later there will be actions that inspire significant public anger. While Han Chinese currently display little or no sympathy for the suffering of Uyghurs, if similarly extensive and intrusive biometric testing, surveillance, and data collection regimes are applied more generally, public attitudes could change.[44]

The greatest paradox is that if the Party displays no trust in its own citizens by employing ever-more intrusive social monitoring and surveillance, the likely result will be even more distrust, leading to unrest, leading to even more monitoring and control — for such are the lessons of escalation in Xinjiang.

This text is taken from *China Story Yearbook: China Dreams*, edited by Jane Golley, Linda Jaivin, Ben Hillman and Sharon Strange, published 2020 by ANU Press, The Australian National University, Canberra, Australia.

doi.org/10.22459/CSY.2020.07