

London Review of Books

Document Number Nine

John Lanchester

The Great Firewall of China: How to Build and Control an Alternative Version of the Internet

by [James Griffiths](#)

Zed, 386 pp, £20.00, March, ISBN 978 1 78699 535 3

We Have Been Harmonised: Life in China's Surveillance State by [Kai Strittmatter](#)

Old Street, 328 pp, £9.99, May, ISBN 978 1 913083 00 7

0:00 / 41:25

Audio: Listen to this article. To hear more, download Audm for iPhone or Android.

The People's Republic of China had its seventieth birthday on 1 October. 'Sheng ri kuai le' to the world's biggest and most populous example of ... of ... well, actually, that sentence is hard to finish. There's no off-the-shelf description for China's political and economic system. 'Socialism with Chinese characteristics' is the Chinese Communist Party's preferred term, but the s-word makes an odd fit with a country that is the world's most important market for luxury goods, has the second largest number of billionaires, stages the world's biggest one-day shopping event, 'Singles' Day', and is home to the world's biggest, fastest-expanding, spendiest, most materially aspirational middle class. Look at the UN's Human Development Index: after seventy years of communist rule, China's inequality figures are dramatically worse than those of the UK and even the US. Can we call that 'socialism'?

It's equally hard to claim China as a triumph of capitalism, given the completeness of state control over most areas of life and the extent of its open interventions in the national economy – capital controls, for instance, are a huge no-no in free-market economics, but are central to the way the CCP runs the biggest economy in the world. This system-with-no-name has been extraordinarily successful, with more than 800 million people raised out of absolute poverty since the 1980s. Growth hasn't slowed down since the global financial crisis – or, as those cheeky scamps at the CCP tend to call it, the Western financial crisis. While the developed world has been struggling with low to no growth, China has grown by more than six per cent a year and a further eighty million mainly rural citizens have been raised out of absolute poverty since 2012. There is a strong claim that this scale of growth, sustained for such an unprecedented number of people over such a number of years, is the greatest economic achievement in human history.

Since Deng Xiaoping instituted the policy of 'reform and opening' in the early 1980s, there has been a general view in the West that the gradual encroachment of capitalism in China would lead to a turn towards democratic government. This reflected a deeply held, largely unexamined belief that capitalism and democracy are interlinked. The collapse of the Soviet Union confirmed the West's victory; an equivalent process would inevitably result in political change coming to China. The 'butchers of Beijing', as Bill Clinton described them in 1992, would be swept away by history. The arrival of the internet made this inevitability seem even more inevitable. 'Liberty will be spread by cell phone and cable modem,' Clinton said. 'We know how much the internet has changed America, and we are already an open society. Imagine how much it could change China.' As James Griffiths tells us in *The Great Firewall of China*, his detailed and compelling account of Chinese online censorship, this was an applause line for Clinton in 2000. 'Now there's no question China has been trying to crack down on the internet,' Clinton went on. 'Good luck. That's sort of like trying to nail jello to the wall.' This perspective on the internet sees it as an informational form of manifest destiny. In the words of the *New York Times* columnist Thomas Friedman, the internet is a 'nutcracker to open societies'. This view has adherents in China too. Liu Xiaobo – the first Nobel laureate to die in prison since Carl von Ossietzky in Nazi Germany – said the internet was 'God's gift' to a democratic China. The celebrity dissident artist Ai Weiwei says: 'The internet cannot be controlled. And if it is uncontrollable, freedom will win. It is that simple.'

The CCP doesn't agree. Its position is the diametric opposite of the Western received wisdom that the internet is necessarily and in its essence a threat to the authoritarian state. The Chinese government favours the doctrine of 'cyber-sovereignty', in which countries have control over their own versions of the internet. Kai Strittmatter was for many years the Beijing correspondent for the *Süddeutsche Zeitung*, and his excellent *We Have Been Harmonised* is an eye-opening account of this issue. ('Harmonised' is a euphemism for 'censored'.)

The days when the party eyed the internet with fear and anxiety are long gone. The regime has not only lost its fear; it has learned to love new technologies. The CCP believes it can use big data and artificial intelligence to create steering mechanisms that will catapult its economy into the future and make its apparatus crisis-proof. At the same time, it intends to create the most perfect surveillance state the world has ever seen.

To understand the Chinese government's view of these matters, the simplest technique is to hold on to that idea of diametric opposites. Gorbachev? 'Gorbachev was once widely praised by the West and his political reform even won much admiration in China,' an editorial explained in the *People's Daily* in 2010. 'But, it was Gorbachev that finally ruined the Soviet Union. Therefore, China must not follow the Western world's practice on crucial issues such as internet control and supervision.' Donald Trump? The *People's Daily* again, via Twitter this time: '@realdonaldtrump is right. #fakenews is the enemy. China has known this for years.' Tiananmen was a disaster for China, no? Au contraire: in Griffiths's words, 'it was argued, even by those who had recognised the horrors experienced in Beijing, that China's

subsequent prosperity and modernity justified the crackdown; that without Deng's firm hand in 1989, he would not have been able to oversee subsequent reforms that led to an economic boom.'

The most important of these diametric opposites concerns Western liberal values. In 2013, an amazing paper from the highest reaches of the CCP, catchily known as 'Document Number Nine', or 'Communiqué on the Current State of the Ideological Sphere', came to light. (The journalist who leaked it, Gao Yu, was sentenced to seven years in prison and is currently under house arrest.) Document Number Nine warned of 'the following false ideological trends, positions and activities': 'promoting Western constitutional democracy'; 'promoting "universal values"'; 'promoting civil society'; 'promoting neoliberalism'; 'promoting the West's idea of journalism, challenging China's principle that the media and publishing system should be subject to party discipline'; 'promoting historical nihilism' (which means contradicting the party's view of history); 'questioning Reform and Opening and the socialist nature of socialism with Chinese characteristics'. The paper, which is cogent and clear, takes direct aim at the core values of Western democracy, and explicitly identifies them as the enemies of the party.^[1] It sees the internet as a crucial forum for defeating these enemies. The conclusion speaks of the need to 'conscientiously strengthen management of the ideological battlefield', and especially to 'strengthen guidance of public opinion on the internet' and 'purify the environment of public opinion on the internet'.

Document Number Nine is thought to have been either directly written by, or under the auspices of, President Xi Jinping. It marked a new turn in the history of China, and quite possibly the history of the world: the moment at which a powerful nation-state looked at the entire internet's direction of travel – towards openness, interconnection, globalisation, the free flow of information – and decided to reverse it. In effect, it was a decision to prove the Western boosters of the internet – holders of Friedman's nutcracker view – wrong.

Between them, Griffiths and Strittmatter tell the story of how China arrived at this point, and what happened next. China took to the internet relatively late and relatively slowly: in 1994 there were only about 1500 internet users in China, most of them academics, with, according to Griffiths, 'the entire country sharing the equivalent of what was a home connection in the US'. Today, the number of internet users in China is 830 million and counting, with most of them accessing it via smartphones. The party has fought many battles against internet freedom over the course of that quarter-century.

The first fights were mainly to do with news, in the form of newsletters such as Da Cankao ('big reference') or news sites such as China Digital Times. Overseas websites such as the *New York Times* and BBC were blocked, and Google was allowed into China on the condition that it censor itself, until the resulting inner torment caused the company to withdraw in 2010. Facebook has never been allowed into China, despite Mark Zuckerberg's increasingly tragic attempts to suck up to the CCP: by prominently announcing that he was learning Mandarin, being photographed jogging in Beijing's reeking, toxic smog, asking Xi Jinping to name his daughter (Xi declined) and – my favourite – making sure he has a copy of Xi's arse-numbingly tedious *The Governance of China* on his desk when Chinese journalists visit

Facebook. ('I've bought copies of this book for my colleagues as well,' Zuck says. 'I want them to understand socialism with Chinese characteristics.')

The biggest internet companies in China can be seen as knock-offs of American originals, though because China is so big, the Chinese versions are now in many cases larger than their US templates, and as they have grown they have added many distinctive features of their own. Baidu is Google, Alibaba is Amazon (they're the ones behind 'Singles' Day'), Tencent is sort of Facebook plus Netflix. These three giants together are known as BAT, analogous to Silicon Valley's FAANG of Facebook, Amazon, Apple, Netflix and Google. Sina Weibo, usually referred to just as Weibo, is Twitter, which has been blocked in China since 2009. The story of the Chinese internet pivots around Weibo, because it was that company that came closest to embodying the opening up of information that internet advocates see as the main transformational point of the technology.

Weibo launched in August 2009 and over the next few years was the site of an unprecedented new freedom for Chinese citizens. People used it to connect and communicate and, increasingly, to complain – about pollution, corruption and government scandals. As Strittmatter puts it, 'for the first time since the People's Republic was founded in 1949, there was a public space that belonged to citizens, where their language was spoken. The germ of a civil society began to grow.' In July 2011, a train derailment on China's high-speed network killed forty people in Wenzhou, but, as Griffiths says, 'did not make the front pages of the following day's national newspapers'. Officials on the scene almost immediately ordered the wrecked carriages to be broken up and buried underground; several hours later a two-year-old girl was found alive in the wreckage, after the official search had been stopped. Weibo users latched on to the story as a symbol of misgovernance. 'This is a country where a thunderstorm can cause a train to crash, a car can make a bridge collapse, and drinking milk can lead to kidney stones,' Griffiths quotes one user saying. 'Today's China is a bullet train racing through a thunderstorm – and we're all passengers.'

Weibo was both a symbol of and a medium for change. 'The Wenzhou train crash was the Weibo generation's coming-out party to the world, showing how, far from being cowed and brainwashed by years of propaganda, young Chinese were sick of corruption and bureaucratic ineptitude, and clamouring for change.' The outrage of Weibo users did not spare the CCP itself. In 2012, another Weibo storm blew up when a party functionary from Shanxi was photographed doing the usual boring party-functionary stuff, while visibly wearing Rolex and Vacheron Constantin watches worth more than \$100,000. 'Watch Brother' symbolised the self-enriching, out of touch, corrupt side of the CCP.

*

This was the context for Document Number Nine, and it was also the point at which the CCP launched its counterattack. First, the Weibo accounts of prominent critics were 'harmonised' – in other words, deleted overnight. Then a conference was called for 'Big Vs', people with well-followed verified accounts, analogous to Twitter's blue tick. At the conference, the newly formed Cyberspace Administration of China reminded the assembled big shots about their 'social responsibility' to the 'interests of the state' and 'core socialist values'. Two weeks later,

on 23 August 2013, the prominent investor and Weibo activist Charles Xue was arrested. He turned up shortly afterwards in a Chinese Central Television interview from his prison cell, weeping and apologising for his irresponsibility and vanity.

Such TV interviews have become a staple feature of the CCP's internet crackdown, helped by a new law, passed in September 2013, which threatens three years in prison to anyone who shares a rumour that 'upsets social order' and is shared five hundred times or clicked on five thousand times. For people with Weibo followings well into the millions, the law effectively banned the posting of anything even potentially controversial. 'Ever since, Weibo has been dead as a politically relevant medium,' Griffiths writes. 'Once, debate had raged there: sometimes wild, often polemical, clever if you were lucky – but always lively. Today, it's as silent as the grave.' Weibo continues to grow, mind you; it's just that it's now the usual entertainment news and celebrity bollocks.

The party's new focus on internet censorship was given its first big test by the Umbrella Protests in Hong Kong, which kicked off in September 2014 – the name comes from the fact that protesters used raised umbrellas to ward off tear gas. The protests drew almost no attention in mainland China, thanks to the blocking of news and messages from Hong Kong, and also thanks to the systematic use of counter-propaganda by a new 'fifty-cent army' of paid bloggers, trolls and subject-changers ('fifty-cent' because that's the amount allegedly paid per helpful post).

The structure for CCP control of the internet was by now fully in place. The popular term for the structure, the Great Firewall of China, is catchy, but as both Griffiths and Strittmatter point out, it's misleading as a guide to how the system actually works. Yes, there is a firewall restricting access to the outside world, and yes, the firewall automatically blocks access to certain sites and certain subjects. Griffiths:

When a user in China tries to load a web page, their ISP pings a list of forbidden URLs and types of content. If the page is not banned, the request is passed to an internet access point which handles routing traffic to servers all over China and around the world. It's at this stage that packet inspection takes place, looking for keywords and suspicious flags. When the destination server sends the webpage data back to the user, it is inspected again. Only if it clears all these hurdles is the internet browser able to load anything.

That is the most firewalled part of the Great Firewall. But it isn't the most important component of the censorship: 'The centrepiece of the Great Firewall is the system of internal controls that operates within the country's borders.' Most Chinese users of the internet focus their use on China, and would barely notice if the rest of the world were permanently cut off. For the censorship and control of the Chinese internet, one of the most useful tools is the app WeChat, which is one of the wonders of the internet world. WeChat – a subsidiary of Tencent – is a chat app similar to WhatsApp, but it also incorporates China's biggest system of payments.^[2] Hundreds of millions of people use WeChat to pay for stuff, do their banking, call minicabs, find movies, book appointments, order takeaways and, of course, to

communicate with one another, via phone or text or social network. No more than five hundred people are allowed to take part in any one chat – you can communicate with your family and your mates, but not broadcast across the entire platform on a Weibo-like scale.

WeChat is WhatsApp plus Uber plus Deliveroo plus Facebook plus online banking, and it is also god's greatest gift to the Chinese surveillance state, since the authorities have access to all this information. People have gone to jail for things they have said in WeChat messages, and the service is penetrated both by targeted surveillance and by the automated blocking of specific terms. There are moments when WeChat exchanges suddenly stop making sense, because messages have been blocked as a result of the algorithmic censorship of particular words; the list of prohibited words changes according to circumstances. When Xi Jinping broke with the term limit system introduced by Deng Xiaoping in 1982, and made himself president for life, Weibo brought in a block on terms such as 'emperor', 'accession', 'don't agree', as well as any reference to *Animal Farm*. 'Winnie the Pooh' is blocked because it has become a metonym for Zuckerberg's hero Xi, who has admittedly put on a couple of pounds since acceding to high office. A man from Shangdong went to prison for 22 months for calling Xi a 'Maoist thug' and 'baozi' – a round dumpling. Tiananmen is an especially touchy subject. Every year around the anniversary, 'that day' is blocked, as is '35 May' (a clever-clogs way of referring to 4 June); so is the word 'mourn'. Baidu Baike, the Chinese version of Wikipedia, says it is 'an open and free online encyclopedia'; it has entries for the years 1988 and 1990 but not for 1989, the year of the protests.

If anything unwelcome does get past the multiple layers of censorship and blocking – more like a Giant Onion than a Great Firewall – it runs into the fifty-cent army, the *wumao*. The effort involved is extensive. An American university study of the Chinese internet counted 448 million fake social media posts in one year, 2016, with the preferred tactic of the fifty-cent army being not to pile on to critics – though they do that too – but to deflect attention, ideally by 'cheerleading' for pro-government news. Griffiths quotes the research:

They do not step up to defend the government, its leaders and their policies from criticism, no matter how vitriolic; indeed, they seem to avoid controversial issues entirely. Instead, most posts are about cheerleading and positive discussions of valence issues. We also detect a high level of co-ordination in the timing and content in these posts. A theory consistent with these patterns is that the strategic objective of the regime is to distract and redirect public attention from discussions or events with collective action potential.

These are the pillars of the Chinese internet: ferocious laws; public humiliation as a tool of coercion; a firewall blocking external sites and independent sources of information; a huge, and hugely expensive, army of censors, backed by algorithms and unprecedented levels of surveillance, adding up to the Giant Onion; and a fifty-cent army of trolls and handwavers to pile on, distract and deflect.

The point of the state apparatus is not to silence all debate, but to prevent organisation and co-ordination; the ultimate no-no is the formation of any kind of non-party group. The CCP's

goal is not silence but isolation: you can say things, but you can't organise. That is why the party has cracked down with such ferocity on the apparently harmless organisation Falun Gong, whose emphasis on collective breathing exercises wouldn't normally, you would think, represent much of a challenge to CCP control of China. But Falun Gong grew popular, too popular – seventy million by 1999, as many as the CCP itself – and had an unacceptable level of collective organisation. So the party set out to destroy it. Two thousand members of Falun Gong have died in custody since the crackdown began.

Given all this, it is frequently the case that outsiders are surprised by the apparent freedom of the Chinese internet. People do feel able to complain, especially about pollution and food scandals. As Strittmatter puts it, 'a wide range of competing ideologies continues to circulate on the Chinese internet, despite the blows struck by the censors: Maoists, the New Left, patriots, fanatical nationalists, traditionalists, humanists, liberals, democrats, neoliberals, fans of the USA and various others are launching debates on forums.' The ultimate goal of this apparatus is to make people internalise the controls, to develop limits to their curiosity and appetite for non-party information. Unfortunately, there is evidence that this approach works: Chinese internet users are measurably less likely to use technology designed to circumvent censorship and access overseas sources of information than they used to be.

*

Technology doesn't stay still, though, and the story of the CCP and the digital revolution will not end here. The party sees its engagement with the net as a success, and plans to make a success of the next stage too. Liu Qiangdong, the boss of JD.com, the world's biggest manufacturer of drones, reports that in 2017 he was thinking about the progress of AI and 'suddenly discovered that communism can actually be realised in our generation'. That might seem a startling claim – indeed, it is a startling claim. But he is in the mainstream of party thinking on this. Big data and artificial intelligence are the next big thing in computing.^[3] The party's plans for it, as set out in the State Council's 'next generation artificial intelligence development plan', published in 2017, are the most ambitious of any government in the world. (It's noteworthy that this paper, which is fully as alarming as Document Number Nine, was freely published by a government press. The CCP is proud of what it has in mind.)

'Digitalisation has brought the Chinese people the historic opportunity of the millennium,' the plan says. What does that mean? It means that China feels that it fell behind the West by missing out on the industrial revolution, and intends not to repeat the mistake with this coming wave of technological change. When it comes to AI the party really, really isn't messing around. 'The widespread use of AI in education, medical care, pensions, environmental protection, urban operations, judicial services and other fields will greatly improve the level of precision in public services, comprehensively enhancing the people's quality of life.' Oh, and by the way: 'AI technologies can accurately sense, forecast, and provide early warning of major situations for infrastructure facilities and social security operations; grasp group cognition and psychological changes in a timely manner ... which will significantly elevate the capability and level of social governance, playing an irreplaceable role in effectively maintaining social stability.' This is as pure a dream of a totalitarian state as there has ever been – a future in which the state knows everything and anticipates everything,

acting on its citizens' needs before the citizen is aware of having them. It is an autocratic fantasy, a posthumanist dream, hiding in the plain sight of a Chinese government white paper.

An early example of what that AI paradise might look like in operation has arrived in the field of facial recognition. This is an area in which increased computing power has delivered a new ability for machines to recognise faces in real time. From the point of view of security and privacy this has been transformational: it means that the people operating the cameras know whom they are looking at right here, right now. The arrival of AI has turned the hundreds of thousands of cameras in our cities from passive recording devices into a connected network offering real-time surveillance and supervision. Add facial recognition to this and we have something new. The cute, customer-friendly side of this is effortless check-in at Chinese airports: the passenger simply stands in front of a camera and is identified, her boarding pass printed, without any action on her part. The slightly less cute version comes, say, in Beijing's Temple of Heaven, where a machine in the toilet, designed to crack down on excessive use of loo paper, 'releases 60 cm of paper per face'; you can get more paper but you either need to grow a new face or wait nine minutes. And then there are the uses which aren't cute at all: a street crossing in Fujian where jaywalkers are identified and have their face, name and address appear on a video screen beside the road; a school in Hangzhou where facial recognition technology monitors students to see when they are bored or distracted (the scanners are also used to pay for food and borrow books from the library); a state surveillance network, Skynet (yes, that's the same as the evil computer system in the Terminator movies), which is capable of identifying any one of China's 1.4 billion citizens within a second. Skynet is part of what's been called the 'police cloud', in which police gather and synthesise all the information they can: 'medical histories, takeaway orders, courier deliveries, supermarket loyalty card numbers, methods of birth control, religious affiliations, online behaviour, flights and train journeys, GPS movement co-ordinates and biometric data, face, voice, fingerprints – plus the DNA of some forty million Chinese people'.

This progress in facial recognition and big data is all part of the other development in the Chinese digital world, the social credit system. This is a credit score analogous to those which are run in the West by credit reference agencies such as Experian and Equifax. The complete view of our lives and finances owned by these firms seems largely to escape attention in the West, but it hasn't escaped the attention of the CCP, which has multiple trials running of social credit systems that build on and expand the existing Western model. The Chinese pilots look not at consumer creditworthiness but at social behaviour, with the criteria for desirable behaviour defined by the party. Strittmatter cites a pilot in Rongcheng, where citizens get points – not a metaphor, they actually are awarded points – for helping aged neighbours move house, giving calligraphy lessons and offering use of their basement for a CCP singalong. Conversely they lose points for pouring water outside their house so it turns into ice, letting their dogs shit on the pavement, driving through red lights and so on. In some versions of these schemes, your social credit is affected by the social credit of the people you hang out with; a bad reputation is contagious.

At the moment, the main impacts of people's social credit are on activities such as travel: people with bad social credit can't fly, can't book high-speed train tickets or sleeper berths; they have slower internet access and can't book fancy hotels or restaurants. It isn't difficult to project a future in which these sanctions spread to every area of life. The China-wide version of social credit is scheduled to go live in 2020. The ultimate goal is to make people internalise their sense of the state: to make people self-censor, self-monitor, self-supervise. Strittmatter quotes *Discipline and Punish*: 'He who is subjected to a field of visibility, and who knows it, assumes responsibility for the constraints of power; he makes them play spontaneously upon himself; he inscribes in himself the power relation in which he simultaneously plays both roles; he becomes the principle of his own subjection.' The Chinese version of social credit is the closest thing we've ever seen to Foucault's system in action at a national level.

Put all this together. Imagine a place in which there's a police post every hundred metres, and tens of thousands of cameras linked to a state-run facial recognition system; where people are forced to have police-owned GPS systems in their cars, and you can buy petrol only after having your face scanned; where all mobile phones have a state app on them to monitor their activity and prevent access to 'damaging information'; where religious activity is monitored; where the state knows whether you have family and friends abroad, and where the government offers free health clinics as a way of getting your fingerprint and iris scan and samples of your DNA. Strittmatter points out that you don't need to imagine this place, because it exists: that's life in Xinjiang for the minority population of Muslim Uighurs. Increasingly, policing in Xinjiang has an algorithmic basis. A superb piece of reporting by Christian Shepherd in the *Financial Times* recently told the story of Yalqun Rozi, who has ended up in a re-education camp for publishing Uighur textbooks in an attempt to preserve the language. One of his crimes was using too high a percentage of Uighur words. The system allows a maximum of 30 per cent from minority language sources; Rozi had used 60 per cent Uighur, and 'China' had appeared only four times in 200,000 words. Uighurs get into trouble for attending mosque too often or too fervently, or for naming their children Mohammed, or for fasting during Ramadan. There are about 12 million Uighurs in Xinjiang: 1.5 million of them have either spent time in a re-education camp or are in one right now.

*

China has been a dictatorship for seventy years. The idea that prosperity and the internet would in themselves make the country turn towards democracy has been proved wrong. Instead, China is about to become something new: an AI-powered techno-totalitarian state. The project aims to form not only a new kind of state but a new kind of human being, one who has fully internalised the demands of the state and the completeness of its surveillance and control. That internalisation is the goal: agencies of the state will never need to intervene to correct the citizen's behaviour, because the citizen has done it for them in advance.

We have no need to reach a conclusion about the prospects for this new China – there's plenty of time for that, and the chance of averting this future for China by wringing one's hands about it is exactly zero. One point which stands out for me, though, draws on Bran Ferren's immortal observation: 'Technology is stuff that doesn't work yet.' In other words, when technology is introduced, it doesn't quite function as it's supposed to; by the time it

really does work, we stop noticing that it is technology and just accept it as part of the furniture of life. With the side of the new technology that concerns 'security', it doesn't necessarily matter whether the surveillance really works or not. Of course, it matters deeply for the individual citizen: facial recognition currently has an error rate as high as 15 per cent; combine that with a judicial system that has a conviction rate of 99.9 per cent and some law-abiding people are going to run into problems. However, from the state's point of view, that matters less than the deterrent and coercive power of omnipresent surveillance combined with social credit. People will change their behaviour because they know they're being watched. It doesn't need to work in order to work.

The other side of the AI revolution is different. The CCP has always used rumblings from below to tell them what people are thinking, and where the party's next problem is coming from – one reason the party likes the internet is because it's a means of finding out what is on people's minds, not just for the purposes of surveillance but for governance too. Precisely because it is authoritarian, the state must listen to its citizens. The idea is to replace the listening system with AI, in order accurately to 'sense, forecast and provide early warning of major situations for infrastructure facilities and social security operations; grasp group cognition and psychological changes in a timely manner'. Great, if it works perfectly. But it won't, because new technology never does. China is facing problems linked to rising inequality. The world's most populous country and leading greenhouse gas emitter (and leading manufacturer of solar technology) is also at severe risk from climate change. This might be the ideal time to experiment with a new kind of government by AI and big data; or not. It is one of the paradoxes of this moment that the world's biggest and most effective dictatorship is taking such a big step towards an unprecedentedly technocratic form of government.

From the perspective of the West, we have a lot to learn from China, in particular about the scale and potential consequences of this new industrial revolution. Much if not all of the technology currently developed in China already exists in the West, in forms that are just as intrusive. The difference is that the technology is almost all in the hands of private companies. AI, big data, facial recognition: Facebook, Google, Amazon, Apple and any number of smaller and emerging companies are deeply invested in these fields. Add what these companies know about you to the colossal amount of data held by the credit reference agencies, and we are as fully open to surveillance in the West as are the citizens of the People's Republic. There is a touch of bathos to this: the technologies which are being used in China to invent a new form of the totalitarian state are being exploited here to make us click on ads and buy stuff.

Facial recognition is as we speak going live all over the developed world, and doing so in a manner that is fragmented, erratic and not at all thought through. Example: the Metropolitan Police has recently been running trials of live facial recognition. One pilot took place in Romford, where cameras were set up to film and identify passersby without their knowledge or consent. Four people were arrested for hiding their faces from the cameras. Is that how we want our policing to work? A London wine bar called Gordon's, well known to anyone who has ever looked for a cheapish and non-horrible place to have a drink in the area around the

Strand, turns up in an *FT* headline: ‘How one London wine bar helped Brazil to cut crime’. Eh? What? It turns out the management of Gordon’s, previously best known for the invention of an oxymoronic ‘pork pie salad’, also came up with a facial recognition system to catch pickpockets and bag-snatchers, many of whom are repeat offenders, and has made money selling the system to shopping malls in Brazil. I mention this not because Gordon’s is an existential risk to democracy but just to make the point that this technology is becoming mainstream, and fast.

The big players in the area are the existing big players in technology, especially Facebook. Do we want facial recognition technology to be in the hands of the least scrupulous technology giant? If we don’t, we’re too late – it already is. Facebook has changed its terms of service over ‘tagging’ people’s photos a couple of times, from opt-out to opt-in, but the gist is that it is too late: Facebook already owns your ‘faceprint’, the algorithmic representation of your face. How much do we think we can trust them with it? Put it like this: Facebook owns a patent on how to recognise patterns of friendship association through identifying the spots of dust on your phone camera – in other words, if two people had their photo taken by the same camera, then those two people probably know each other. That’s important to the company, because the ‘People You May Know’ feature is one of Facebook’s strongest drivers of growth and engagement. Facebook also owns a patent on a system that interprets people’s facial expressions as they walk around a shop looking at the merchandise, and another on a system that recognises shoppers’ faces and assigns them a ‘trust level’ derived from their Facebook profile. The trust level might unlock special deals, if it were positive, but if it were negative – who knows? Why on earth would we trust Facebook?

The risk for the developed world is that all the apparatus of surveillance and manipulation that the CCP is developing as a matter of deliberate policy, we develop inadvertently, and end up adopting through negligence, or nescience, or because we’re thinking about other things. In 2013, at the behest of Alan Rusbridger, I spent a week reading the Snowden papers that the *Guardian* had to destroy in the UK but kept a copy of in New York. They provided a striking portrait of the security services’ attitudes to the huge boon given them by new technology. After all, it wasn’t as if democracies collectively decided to give the security services an exponentially greater and ever growing level of access to their citizens’ private lives. It was just that new technologies came along and changed the way people lived, and those changes just happened to open their lives up to new levels of surveillance and scrutiny. This new bounty just fell into the lap of the secret services, and they accepted it gleefully.

That’s how it would be with facial recognition and AI and big data too. It wouldn’t be a Dr Evil move on the part of Western democracies to access all the new information; they would just take it because it was there, because it suddenly became available. And this, I think, is something we can’t allow to happen. In the developed world, the discourse around the internet is beginning to shift away from the idea of a deregulated, extra-governmental space and to acknowledge the need for legislation and accountability. China has repeatedly done the diametric opposite of us; this time we should live up to the values excoriated by Document Number Nine, and do the exact opposite of them. We should take China’s example seriously, and learn from it, and begin with a complete ban on real-time facial recognition. We should

retain that ban unless and until we understand the technology and have worked out a guaranteed way of preventing its misuses. And then we need to have a big collective think about what we want from the new world of big data and AI, towards which we are currently sleepwalking.

[1] Consider the bit about neoliberalism: ‘Neoliberalism advocates unrestrained economic liberalisation, complete privatisation and total marketisation, and it opposes any kind of interference or regulation by the state. Western countries, led by the United States, carry out their neoliberal agendas under the guise of “globalisation”, visiting catastrophic consequences upon Latin America, the Soviet Union and Eastern Europe, and have also dragged themselves into the international financial crisis from which they have yet to recover.’ ¡Ole!

[2] Pony Ma, head of Tencent, wanted to buy WhatsApp, but had to go into hospital for a back operation before the deal was complete; Zuckerberg rushed in with a bid of \$19 billion while Ma was away from his desk.

[3] I prefer the term ‘machine learning’ to ‘artificial intelligence’ for two reasons: first, it seems to me to be a more accurate description for algorithms which are designed to suck up huge amounts of data and learn from that data to improve their own functioning; second, ‘artificial intelligence’ has all sorts of distracting associations with robot takeovers and independent cognition and suchlike. We can worry about AI when it is closer to hand, is my view; what we are facing at the moment is an explosion in machine learning. However, the CCP and the books under review talk about AI, so AI it is.

[Vol. 41 No. 19 · 10 October 2019](#) » [John Lanchester](#) » [Document Number Nine](#)
pages 3-10 | 6491 words