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

5

AI DREAMS AND AUTHORITARIAN NIGHTMARES

Olivia Shen

IN JULY 2017, the State Council of the People's Republic of China (PRC) announced its ambitious plan to lead the world in the development and application of artificial intelligence (AI). China aims to become the global centre for AI innovation by 2030. Government agencies have released five strategic papers in recent years articulating how AI will profoundly change human society and stressing the importance of harnessing its potential.[1]

China's ministries, local authorities, companies, and the scientific and academic communities are underwriting its AI ambitions through extensive financing and political support. Meanwhile, state media is helping popularise AI in the public consciousness, linking it to China's continued prosperity and modernisation. Citizens are starting to see the benefits of AI throughout the economy, from smart devices and robots that provide daily conveniences to autonomous vehicle trials easing congestion in major cities. Unsurprisingly, the Chinese are more optimistic than other nationalities about the potential for AI to do good.[2] They also appear to be confident in China's AI capabilities, with fifty-five percent believing they are already leading or leapfrogging ahead of other countries in AI development.[3]

The Dark Side of AI

On the darker side of China's AI ambitions are efforts to harness AI for public security. The Chinese government has not been shy about experimenting with AI for authoritarian ends. This is starkly evident in Xinjiang province, where the government's Strike Hard Campaign 严厉打击暴力恐怖活动专项动 is turning Xinjiang into a testing ground for the use of innovative technologies for social control. Facial recognition, machine learning, natural language processing, and genetic profiling allow authorities to keep the community in check with unprecedented efficiency, scale, and secrecy. More than one million Uyghurs and Kazakhs have been sent to 'political education' camps, many of them arbitrarily detained for activities that are by no means illegal under Chinese law[4] (see Chapter 7 'Schemes, Dreams and Nightmares: China's Paradox(es) of Trust', pp.199–211).

To domestic constituents, China's government promotes AI as an accurate scientific tool for monitoring and preventing security threats and unrest. The State Council's 2017 New Generation Artificial Intelligence Development Plan declares:

> 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; and take the initiative in decision-making and reactions — which will significantly elevate the capability and level of social governance, playing an irreplaceable role in effectively maintaining social stability.[5]

This faith in AI may be misguided. As the saying goes, 'Garbage in, garbage out'. If an AI system is built on biased assumptions or poor data, it is likely to codify existing prejudices and inequalities or generate inaccurate results.

Relying on AI in security and law enforcement settings can have its pitfalls. In London, recent trials of live facial recognition by the Metropolitan Police produced inaccurate matches ninety-six percent of the time.[6] In the United States, AI algorithms deployed to predict crime have discriminated unfairly against African Americans because the systems are trained using historical crime data collected by police with a record of targeting minorities.[7] Biased AI systems are prone to error, overlooking or misidentifying security threats because the algorithms have been trained to look for the wrong indicators. In the Strike Hard Campaign, authorities are directed to collect information about suspicious individuals. However, many of the behaviours that are deemed suspicious are either integral to the Islamic faith (for example, collecting money for mosques, going on *Hajj*) or innocuous activities (curiously including welding and using too much electricity, as well as spending time abroad).[8] Such inherent biases create a pernicious feedback loop. Muslims, welders, and frequent flyers are more likely to be flagged as security threats and investigated, which then validates subjecting these groups to even more invasive monitoring. Far from being neutral tools, algorithms are what AI ethicist Cathy O'Neil calls 'opinions embedded in code'.[9]

The Chinese government has a vested interest in presenting AI as scientific, precise, and unimpeachable. If it portrays AI as an objective guarantor of security and other public goods, its citizenry can trust that AI will only harm those individuals who deserve it — criminals, terrorists, separatists, cheats, and other social undesirables. This narrative has been powerful in justifying mass surveillance. China's first national video surveillance program, Skynet 天网, is based on a Chinese idiom about the inescapability of justice (天网恢恢, 疏而不漏 — 'heaven's net is wide, but nothing escapes it'). State media calls the system 'the eyes that safeguard China' and claims it has helped police make numerous arrests.[10] Ironically, 'Skynet' is the name of the superintelligence in *The Terminator* movies that is intent on destroying humankind. China's Skynet is no killer robot, but the potential for repressive uses of AI is growing as Beijing rapidly expands its surveillance apparatus and access to citizens' data.

Big Data Gets Bigger

From 2020, two programs due for completion will combine to collect and aggregate a massive trove of information about Chinese citizens, their movements and their behaviours. The first is Skynet's successor, Sharp Eyes 雪亮 (literally, 'snow-bright'), which will blanket all key public places

Surveillance Cameras
Source: Pixabay

and major industries with live surveillance cameras.[11] Like Skynet, the name of the program is deliberate and symbolic. 'Sharp Eyes' derives from a Cultural Revolution–era saying, 'the eyes of the masses are bright as snow' 群众的眼睛是雪亮的, which encouraged people to snitch on political subversives. It is a chilling reminder of a time when neighbours and relatives denounced one another for party disloyalty[12] (see also Chapter 2 Forum 'Xi Jinping's War on "Black and Evil"', pp.43–46).

The year 2020 will also see the national rollout of the Social Credit System that tracks the trustworthiness of companies, government agencies, and citizens. Social credit metes out punishments and rewards based on compliance with government regulations and court orders, among other metrics for good citizenship. The worst offenders are added to a blacklist; the most compliant are added to a 'red list'. The system requires regulatory agencies and companies to frequently update information to the lists.[13]

Authorities can also request access to the data that companies collect in the course of delivering products, services, content, and advertising to their customers. Research by the US-based Center for Data Innovation suggests that consumer data quantity is one of the few crucial areas for AI development where China already has an advantage over the United States.[14] This is partly thanks to China's lead in mobile payment technologies. With an estimated forty-five percent of the Chinese population using mobile payments, including on omniscient applications such as WeChat, information is continuously being digitised as people go about their daily lives. Companies such as Tencent, owner of WeChat, vacuum up data about what people buy, how they communicate, where they travel, the news they read, the charities to which they donate, and the games they play.

Data collection is also increasingly global. Companies such as Global Tone Communication Technology, an offshoot of the Central Propaganda Department, boasts that it gathers ten terabytes of unstructured global data (equivalent to 4,000 hours of high-definition video streaming) through its media monitoring business each day.[15] The Chinese Academy of Sciences

estimates that China will hold twenty percent of global data, or forty-four billion terabytes, by 2020.[16]

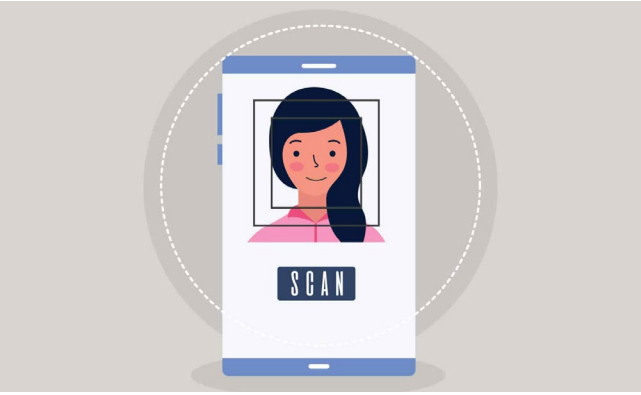
Push for Privacy

In an increasingly data-driven and surveillance-rich world, citizens in many countries are demanding more privacy and transparent uses of their personal information. In 2018, Europe passed the General Data Protection Regulation (GDPR) to enshrine protections for personal data including a right to be free from 'automated processing' by algorithms. The United States is also debating federal data privacy laws, with some states, such as California, pushing ahead with their own versions of the GDPR.

China is grappling with similar concerns and challenges. It is a common misconception that China is devoid of privacy debates or protections. Many netizens were outraged when Baidu founder Robin Li 李彦宏 claimed in 2018 that Chinese were less sensitive about privacy and would exchange privacy for convenience or efficiency.[17] Following a series of high-profile data breaches and scams, citizens have called for stronger privacy laws in recent years.

The government has responded to those calls, but in a manner that targets unscrupulous businesses while maintaining its own access to citizens' data. In 2016, the National People's Congress adopted the Cyber Security Law, which bans online service providers from collecting and selling users' personal information without consent. A 2018 Personal Information Security Specification, modelled on Europe's GDPR, further establishes national standards for seeking user consent and collecting, storing, and sharing personal data.[18] So far, the new regulations have been strictly enforced, with government watchdogs cracking down on smartphone applications that illegally or excessively collect users' data.[19]

While companies are constrained from violating people's privacy, the same cannot be said for the government itself. The very Cyber Security Law



Facial recognition is now commonplace in China
Source: batuhan demirtas, Flickr

that offers better consumer protections also stipulates that online platforms must provide technical support and assistance to government agencies for the purposes of safeguarding national security and investigating criminal activities.[20] China's national security laws, particularly the 2017 Intelligence Law, invest security agencies with sweeping powers to ensure that companies cooperate with intelligence work. The Cyber Security Law further cements those powers. New e-commerce laws that took effect in January 2019 also require e-commerce operators to provide data to the authorities when requested, validate users' real identities, prevent illegal content or activity online, and retain transaction information for no less than three years.

The government throws the book at companies that misuse their customers' data or breach their privacy. However, it shows few signs of curbing its own data mining, surveillance, and censorship capabilities, and advances in AI are rapidly expanding those capabilities. The kinds of technologies seen in Xinjiang are becoming the new normal across much of China. Cities such as Suzhou and Weihai have launched 'police cloud' 警务云 databases that use machine learning to parse massive volumes of data about residents for crime prevention and prediction.[21] Facial recognition is now so commonplace it is used for shaming jaywalkers and dispensing toilet paper in public toilets.[22] Meanwhile, the Cyberspace

Administration will soon require social media algorithms to steer users towards online content that promotes 'mainstream values' such as party policies and Xi Jinping Thought.[23]

From Privacy to AI Ethics

Advances in AI have deepened Chinese concerns about privacy and data. In the 2018 China Economic Life Survey 中国经济生活大调查, jointly run by Tencent's research arm and state media, almost eighty percent of respondents said they thought some applications of AI would compromise their privacy. More than thirty percent also worried that AI would threaten their livelihoods.[24]

In an effort to boost public trust, the government has made a range of commitments to build AI that is ethical and beneficial for society. The State Council's New Generation AI Development Plan includes a goal to establish laws, regulations, and ethical norms for AI by 2025. Beijing has joined the international effort to develop technical AI standards that will also grapple with ethics and safety risks.[25] In May 2019, the Beijing Academy of Artificial Intelligence and the Chinese Ministry of Science and Technology released the 'Beijing AI Principles', which call for AI to be responsible, diverse, open, and beneficial for humanity.[26] The principles carry the endorsement of Peking University, Tsinghua University, the Chinese Academy of Sciences, and China's largest tech firms, including Tencent, Baidu, and Alibaba. Encouragingly, the Beijing Principles are broadly consistent with other AI ethics frameworks recently agreed by the Organisation for Economic Co-operation and Development (OECD) and the G20.[27]

These positive signs of China's engagement on AI ethics contrast with China's aggressive use of the same technologies to manage, and in some cases repress, its own people. Yet for China, there is no contradiction. Social management and safeguarding internal security are part and parcel

of the AI dream. According to the party line, to eschew the capabilities of AI would in fact be unethical. But even if the Chinese population accedes to this argument, international observers are far more sceptical.

International 'Techlash'

One risk for China is that its use of authoritarian AI leads to an international backlash that stunts its AI ambitions. Western media coverage over the past year has highlighted China's human rights abuses in Xinjiang and Hong Kong, with growing emphasis on the role of technology in enabling those abuses. The ongoing scrutiny has prompted some players in the AI field to restrict research and technology transfers.

In October 2019, the United States added twenty-eight Chinese firms to a list of entities barred from buying American products and components, citing human rights concerns. According to the US Department of Commerce, the new listings specifically target firms involved 'in the implementation of China's campaign of repression, mass arbitrary detention and high-technology surveillance against Uyghurs, Kazakhs, and other members of Muslim minority groups'.[28] This includes companies such as Hikvision, Dahua, Yitu, and SenseTime — some of the world's largest manufacturers of video surveillance products.

Hikvision: of the world's largest manufacturers of video surveillance products
Source: Raysonho, Wikipedia

This is the first time human rights have been explicitly declared a US foreign policy interest resulting in the listing of entities.[29] Some speculate the entities listing was motivated more by US trade war tactics than by genuine human rights concerns, coming as it did on the eve of trade negotiations. Nevertheless, the move amplifies concerns about working with China on new technologies. After employee protests, Google terminated a project to build a censored version of its search engine for the Chinese market.[30] Bad publicity also forced American company Thermo Fisher to cease selling DNA sequencers to authorities in Xinjiang for genetic mapping.[31]

Ethical considerations are complicated by the fact that many AI technologies are 'dual use'. Beneficial and harmful AI can be almost indistinguishable at a technical level. Prominent American geneticists who have shared DNA samples with China's Institute of Forensic Science have subsequently discovered that their research was used for genetic profiling.[32] Australian universities have also been implicated, with the University of Technology Sydney and Curtin University forced to review their research approval processes after their academics were involved in projects that may have aided Chinese government surveillance.[33]

Despite impressive investment and progress in indigenous AI development, China still needs global supplies of AI talent and knowhow. With the onset of the China–US trade war, Beijing is particularly sensitive to the risk of overreliance on US producers for critical technological inputs. Crucially, China has not yet succeeded in establishing a local semiconductor industry to produce the chips that power AI computing.[34] China is also still catching up to the United States and others — albeit rapidly — in terms of quality patents, fundamental research, and attracting international expertise. China files more patents, for example, than any other country but only thirty-seven percent are maintained after five years.[35] Programs such as the Thousand Talents 千人计划 have not been able to attract the best and brightest scientists and academics to return to China in the long term.[36] Human rights and reputational concerns are likely to further deter

foreign talent from working with Chinese firms, conducting joint research, investing in Chinese companies, or sharing data, all of which will also slow the pace of China's AI development.

The government's continued use of authoritarian AI also undermines the credibility of its efforts to influence global standards and governance. It is difficult to imagine countries welcoming China to the global negotiating table while millions of Uyghurs remain in detention. It is equally difficult to imagine China coming to the table for meaningful negotiations with other countries that publicly criticise its human rights record and cut off its supply chains. There are concerns, too, that China is rapidly exporting its authoritarian AI to at least fifty-four countries, frequently packaging the technology into the Belt and Road Initiative.[37]

A Comfortable Panopticon

China's burgeoning ocean of data, combined with its growing AI capabilities, generates new opportunities and temptations for social control. If China looks set to continue pursuing more authoritarian applications of AI, one key question is how its citizens might respond. Will there come a tipping point where they object?

Mural by graffiti artist Banksy in London, 2007
Source: ogglog, Flickr

Ordinary Chinese are not naive. Aware that Big Brother is watching, they tend to moderate their behaviour accordingly. An interesting example of this is the case of Tay, Microsoft's AI chatbot that notoriously began posting inflammatory and offensive tweets just hours after it was launched in 2016. Tay was first tested as Xiaoice 小冰 in China, where it gained a strong following over eighteen months with

no such off-script moments. One reason for this difference is that Chinese netizens closely follow online rules. They generally do not harass, smack talk, or troll each other because there is always the possibility that the state is listening in.[38] The online environment thus resembles English philosopher Jeremy Bentham's concept of a 'panopticon' — a prison in which the inmates never know whether they are being watched and are therefore motivated to act as though they are always being watched.

A panopticon might sound chilling to some, but for others it is a comfort. Decades of Communist rule have inured much of the population to government intrusion while coopting them with its benefits. China has a deeply embedded and historical tradition of promoting good moral behaviour. Where fraud, corruption, and cheating are rife, systems that bolster trust and deter wrongdoing are considered necessary and even welcome.[39] Social credit, for example, is far more controversial outside China than within. The Party-state encourages all its citizens to contribute to systems of community policing. In many rural locations where Sharp Eyes is piloted, locals can tune into the live surveillance feeds and report their neighbours' transgressions.[40] Hebei province has released a 'debtor map' 老赖地图 app that allows users to blow the whistle on wealthy-looking debt dodgers in their vicinity.[41]

Many Chinese accept automated monitoring as a small price to pay for stability, prosperity, and social harmony. Those who follow the rules reap the spoils of an ascending China. Those who step out of line pay the costs. China's dreams of AI development are inextricably linked with the use of AI as a tool for social engineering. If China should succeed at both — vastly expanding its AI capabilities and universally deploying those capabilities towards controlling its citizens — its AI dream could turn into a nightmare for any who dare to dissent.

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.2020.05