Australia-China Relations Institute
澳中关系研究院

Opinion

Turning ghosts into humans: Surveillance as an instrument of social engineering in Xinjiang

Michael Clarke
November 2 2021

Note: This article appeared in *War on the Rocks* on November 2 2021.

Wrists and ankles strapped into a restraining 'tiger chair,' a man is used as a subject with which to 'train' artificial intelligence-assisted facial recognition technology to detect states of emotion. Minute changes in facial expression are analyzed by the facial recognition technology to determine whether the test subject possesses a 'negative mindset' or a heightened state of anxiety, allegedly indicating a potential for anti-social behavior. This is not a vision from a dystopic television series.

On the contrary, this is a lived reality in the Xinjiang Uyghur Autonomous Region in the far north-west of China, where the Chinese state, in concert with a number of China's major surveillance technology companies, has striven to perfect new means of monitoring the region's Uyghur population. Researchers estimate that, between 2016 and 2019, up to one million people in the region had been detained without trial in a system of 're-education' camps. In addition, between 2017 and 2020, 533,000 people were formally prosecuted for a variety of 'crimes' under broad definitions of 'extremism' and 'terrorism.'

Outside of the camps, the region's Turkic Muslim populations are also subjected to a dense network of high-technology surveillance systems, checkpoints, and interpersonal monitoring, which severely limit all forms of personal freedom and enhance the state's hold over society. This intense surveillance has led some to describe Xinjiang as a 21st-century police state.

Why did China launch this campaign of repression?

Control of the region's Uyghur population is only part of the objective. The manner in which the system of pervasive surveillance intersects with the Chinese Communist Party's practices of ideological re-education in Xinjiang demonstrates that China has embarked on a program of mass social reengineering to 'remake' Uyghurs and other Turkic Muslims into pliable citizens. Xu Guixiang, a spokesman for the Xinjiang Uyghur Autonomous Region government, asserted on May 25, 2021 that the re-education system was required in order to 'remove extremist thoughts' from Uyghur minds and 'transform' them from 'ghosts' into 'humans.'

This statement serves as a reminder that surveillance is but a means to an end — the protection or management of either the population at large or a specific segment thereof. Indeed, as James C. Scott has argued, a characteristic objective of the modern state has been 'to reduce the chaotic, disorderly, constantly changing social reality beneath it to something more closely resembling the administrative grid of its observations,' rendering citizens and the spaces which they inhabit more transparent to the 'gaze' of the state and thus more responsive to central manipulation and control.

Surveillance is therefore central to a state's capacity for 'social sorting.' Simply, social sorting comprises the 'identification and ordering of individuals in order to 'put them in their place' within local, national and global ‘institutional orders.’ Such a process also enables the state to ascribe to individuals or communities particular penalties, constraints, or sanctions according to their categorization.

The surveillance apparatus erected in Xinjiang has played just such a role by enhancing the state’s control over the Uyghur population and other Turkic Muslims, and its ability to identify those suspected of aberrant behavior and funnel them into the re-education system for ‘transformation.’ From the use of facial recognition and iris scanners at checkpoints, train stations, and mosques to the collection of biometric data for passports to mandatory apps to ‘cleanse’ smartphones of ‘subversive’ material, the surveillance apparatus collects massive amounts of data on ordinary citizens. The data collected is then aggregated by an app security personnel use, the Integrated Joint Operations Platform, to report ’on activities or circumstances deemed suspicious’ and to prompt ‘investigations of people the system flags as problematic.’

How the Party talks about its surveillance apparatus

A closer examination of the legislative and discursive architecture that has been built around the surveillance apparatus reveals how precisely the authorities in China decide who is problematic or, more often, ‘untrustworthy.’

First, in December 2015, the National People’s Congress passed China’s first national ‘anti-terrorism’ law, providing an expansive and ambiguous definition of terrorism:

> Any advocacy or activity that, by means of violence, sabotage, or threat, aims to create social panic, undermine public safety, infringe on personal and property rights, or coerce a state organ or an international organization, in order to achieve political, ideological, or other objectives.

Second, the Xinjiang Uyghur Autonomous Region government announced in March 2017 its so-called ‘de-extremification’ regulations that revealed the state’s objective to categorize and punish those it defines as ‘deviant’ and ‘abnormal.’ These regulations not only define ‘extremification’ as ‘speech and actions under the influence of extremism, that imbue radical religious ideology, and reject and interfere with normal production and livelihood’ but also explicitly identify fifteen ‘primary expressions’ of ‘extremist thinking.’ These include ‘wearing, or compelling others to wear, gowns with face coverings, or to bear symbols of extremification,’ ‘spreading religious fanaticism through irregular beards or name selection,’ and ‘failing to perform the legal formalities in marrying or divorcing by religious methods.’ The regional government subsequently expanded the list in 2017 to include another 60 signs of ‘extremism’ including ‘suddenly quitting smoking or drinking, abnormal communication with neighbors, and men having long beards or wearing short-legged pants.’

Together, these measures amount to what Joanne Smith Finley calls a criminalization of ‘all religious behaviors, not just violent ones,’ leading ‘to highly intrusive forms of religious policing’ that violate and humiliate Uyghurs. Such legislation demonstrates that, for the Chinese Communist Party, everyday markers and practices of the Uyghur identity, such as religion and language, are inherently extremist. Meanwhile, the State Council Information Office of the People’s Republic of China’s White Paper of Aug. 16, 2019, on ‘Vocational Education and Training in Xinjiang’ highlighted the core objective of the Chinese Communist Party to define and regulate Uyghur values, beliefs, and loyalties so that they become ‘useful’ subjects for maintaining the regime’s political security.

Extremism and re-education

While defining ‘terrorism and extremism’ as ‘common enemies of human society,’ with Xinjiang as the ‘main battlefield of China’s fight against terrorism and de-extremization,’ the White Paper also asserted that the state must not only deal with ‘terrorist crimes in accordance with the law’ but also ‘educate and rescue’ those infected with religious extremism in order to treat ‘both symptoms and the root causes’ of religious extremism. Through education and training, the document asserts, the ‘training centers’ will promote development and increase the people’s overall income and help Xinjiang ‘achieve social stability and enduring peace.’

However, it is a 52-gigabyte internal police dataset from the Urumqi Public Security Bureau in the region’s capital, obtained by the *Intercept* and analyzed in detail by Darren Byler, that perhaps best demonstrates both the granular nature of everyday surveillance in Xinjiang and how it intersects with state-defined notions of ideological deviancy and extremism that mark individuals for re-education.

Beginning in 2013, the Urumqi Public Security Bureau began experimenting with mobile scanning devices that integrated 3G mobile technology, smart phones, and virtual private network-enabled databases ‘to allow rapid individual identity authentication.’ By 2017, this technology had been upgraded to allow police in Urumqi to scan and read identification cards, ‘instantly linking ID numbers, issuers, and photos’ of the individual being checked to the Integrated Joint Operations Platform. These ‘social incident reports’ — some 250 million rows of data in the files obtained by the *Intercept* — ‘list the geolocation, date, and time of the encounter, the precinct, name, ID number, gender, ethnicity and phone number of the suspect. They describe the reason why the individual was flagged and if they warrant further investigation.’ The Public Security Bureau used this data to monitor Urumqi’s Uyghur (and Kazakh) population, subjecting them to regular security checks, household searches, monitoring of familial and community relationships, and mosque attendance.

Crucially, the data from the Urumqi Public Security Bureau files also demonstrate that the authorities trained the technology to identify and aggregate actionable intelligence based on ideologically defined criteria. The Urumqi Public Security Bureau’s hand-held mobile scanning devices were armed with a ‘digital forensics’ tool — referred to as a ‘Anti-Terrorism Sword’ — that permitted Public Security Bureau personnel to access ’private social media, email and instant messaging applications to assess the phone owner’s digital history and social network.’

All of these data points have been used to flag an individual for further investigation or detention. A weekly report of one Public Security Bureau precinct in Urumqi in February 2018 notes that it detained 669 people on such a basis and subsequently sent 184 to re-education. This makes it clear that the monitoring of everyday life in Uyghur neighborhoods is geared toward identifying and responding to what the Chinese Communist Party has defined as key markers of ideological deviancy. The surveillance apparatus, and its accompanying processes of ‘social sorting,’ are therefore fundamental to the Chinese Communist Party’s project of not only controlling but remaking Xinjiang’s Uyghur population into ‘productive’ and pliable citizens.

A trend with global origins and global implications

Yet, it is important to also recognize that the Chinese Communist Party’s implementation of this surveillance-enabled form of what it calls counter-terrorism has not taken place in a vacuum. Rather, it is part of the globalization of ‘countering violent extremism’ strategies and discourses that ‘aim to reduce violent extremism by using methods beyond the use of military force and the coercion available under criminal law’ to ‘prevent the emergence of violent extremism before it has fully emerged in a region, community, or an individual, by addressing the underlying factors that give rise to it.’

What is unique about the Chinese manifestation of this countering violent extremism mania is how the surveillance technologies noted above have enabled the Chinese Communist Party to undertake mass social sorting in pursuit of the ideological goal of breaking what it perceives to be the integral link between markers of Turkic Muslim religious and cultural identity, on the one hand, and extremism on the other.

There are a number of important implications flowing from Beijing’s use of this technology-heavy surveillance apparatus, not only for its governance of Xinjiang, but also for China as a whole and the global spread and normalization of such surveillance. With respect to the governance of Xinjiang and the People’s Republic of China, the system erected in Xinjiang potentially sets China on the path to becoming what Xiao Qiang calls a ‘responsive tyranny,’ in which digital technologies empower the state to act preemptively and to identify and quash opposition in advance on the basis of clues gleaned from its many channels of mass information collection.

This technologically enabled system of surveillance and control also intersects with global dynamics in a number of key ways. First, states around the world are increasingly deploying specific technological innovations, such as DNA sequencing, metadata analysis, facial recognition technology, machine learning, and ‘automatic gait recognition‘ in the name of public safety and, especially, counter-terrorism. As Sheena Greitens has documented, the spread of Chinese surveillance and technology platforms to over 100 countries — of all regime types — is ‘not solely driven by China or Chinese companies, but by recipient demand.' This trend arguably makes it both easier for the Chinese state to construct a justificatory narrative around its system of control, and for the state's various security apparatuses and bureaucracies to engage with, and learn from, international partners.

Second, the Chinese state's engagement with, and prioritization of, surveillance technologies has resulted in the increased direct involvement of a number of Chinese technology companies in the provision of both technology and components to the security state in Xinjiang. Chinese video surveillance companies Dahua, Hikvision, Yitu, Megvii, SenseTime, Yixin Science and Technology Co. Ltd., and voice recognition firm iFlytek, for instance, have been heavily involved in providing not only hardware for the surveillance apparatus but in developing and marketing new instruments of surveillance for the state such as ethnicity analytics software that distinguishes Uyghurs from others.

The system of pervasive surveillance, combined with the practices of re-education in Xinjiang, represent an extreme example of the deeply dystopic potentialities of modern ideologies and technologies of social control. The international community should guard against the spread and normalization of such a surveillance-industrial complex through appeals to counter-terrorism imperatives because, as the case of Xinjiang demonstrates, it constitutes an insidious assault on basic norms of human rights.

Can the United States do anything?

One way in which the Biden administration can push back against the normalization of surveillance for social control is by undertaking a concerted effort to track the interconnections between the surveillance apparatus in Xinjiang and Chinese and foreign technology companies. Two potential types of pressures could be leveraged by the U.S. government here: (1) limiting the ability of Chinese companies and entities to access components from U.S.-based companies and, (2) publicly reporting the supply chain connections between Chinese and U.S. companies.

In October 2019, the Trump administration, via the U.S. Department of Commerce, began to undertake the first of these by adding a number of major Chinese technology companies implicated in the surveillance apparatus in Xinjiang — such as video surveillance companies Dahua, Hikvision, Megvii, Yitu, Sensetime, and voice recognition firm iFlytek — to the Bureau of Industry and Security's Entity List. This was a means of limiting their ability to obtain components from U.S. technology giants such as Intel and Nvidia that have been crucial to the development of China's surveillance state.

Restricting implicated Chinese companies' access to U.S. technology, however, is an imperfect solution as such companies have simply sourced supply chain alternatives or are investing heavily to boost their own research and development capabilities to fill the gaps. The Biden administration should undertake a systematic tracking and reporting of supply chain connections between Chinese companies on the Bureau of Industry and Security Entity List and U.S. technology companies. Publishing this information will increase the prospect of reputational risk for U.S. companies by making public their conscious or unconscious complicity in Xinjiang's surveillance state.

One of the central controversies regarding the Chinese Communist Party's systematic repression of the Uyghurs and other Turkic Muslims concerns the question of intent. Has it cynically manipulated the global prioritization of counter-terrorism as a cover to eliminate the very possibility of future resistance to the party-state in Xinjiang? Or does it seek the ultimate dissolution of the Turkic Muslim other?

Scholars will continue to parse the evidence regarding the Chinese Communist Party's ultimate intent for some time to come, but it is now beyond question that technology-enabled surveillance has made possible the mass social sorting — the identification, categorization, and ascription of sanction to individuals — which is central to the 'reeducation and transformation' system. As such, it stands not only as an example of the scope of the Chinese Communist Party's ambitions for social control but also as a warning to other societies as to the deeply dystopic potentialities of the surveillance-industrial complex.

Dr Michael Clarke is a Visiting Fellow at the Australia-China Relations Institute at the University of Technology Sydney.