USCIRF Virtual Hearing on Technological Surveillance of Religion in China

Written Testimony
July 22, 2020

Chris Meserole, Ph.D.
Brookings Institution

Chairwoman Gayle Manchin, Vice Chair Tony Perkins, and Vice Chair Anurima Bhargava,

Thank you for the opportunity to speak this morning. The rise in digital authoritarianism and corresponding decline in human rights, including the right to worship freely, are two of the most pressing issues the world faces today. Nowhere do those issues enjoy greater urgency than in modern China, where the Xi regime and Chinese Communist Party (CCP) have relied on digital technologies to carry out human rights abuses and curtail religious freedom with unprecedented efficiency and scale.

Digital Authoritarianism & the CCP

Before turning to the Xi regime and religion, I should first lay out what I mean by digital authoritarianism more broadly. As with all political regimes, authoritarian leaders are obsessed with their survival. Yet staying in power is not easy: regimes need to closely monitor not only elite opinion and public opinion, but also potential dissidents and opposition groups. Digital technology offers a new way to solve that challenge. As the cost of storing, collecting, and analyzing data has plummeted, the capabilities of digital surveillance systems have grown exponentially. Regimes with sufficient technical expertise can now monitor both aggregate opinion and specific individuals with greater precision and detail than ever before. Digital authoritarianism refers to the use of such technologies to consolidate regime power and better ensure regime survival.

No authoritarian state has leveraged digital technologies more successfully than modern China. Dating back to the early 1980s, the CCP has consistently taken a two-pronged approach to information technology. On the one hand, they have aggressively cultivated and fostered a domestic technology industry in the pursuit of economic growth. On the other, the CCP has erected an elaborate infrastructure for monitoring and surveilling the domestic use of digital platforms. Forty years later, the strategy has proven a resounding success. China is now a world leader not just in the manufacture of commodity hardware and electronics, but of cutting-edge technologies like artificial intelligence. At the same time, domestic programs like the Great Firewall and Sharp Eyes have given the CCP censorship and surveillance capabilities far in excess of what they enjoyed previously. Rather than leading to greater political openness and instability, the CCP's push into information technology has provided the party with powerful and unprecedented new tools for surveilling the speech and behavior of its citizens.

For religious groups targeted by the CCP, the result has been as devastating as it is tragic.

Digital Authoritarianism and the CCP's Repression of Religion

After the religious purges of the Mao era, the CCP Central Committee famously loosened restrictions on religious practice in the early 1980s with the issuance of Document 19. Yet the CCP nonetheless continued to view many religious communities as a threat, particularly those it believes to have ties with co-religionists abroad. In the time since, the party has typically dealt with that threat through a twofold strategy of Sinicization and repression.

Digital technologies have rendered that repression far more effective. As with authoritarians elsewhere, the CCP has long been able to repress public forms of religious organizations, practices, identities, and beliefs, particularly in urban areas. But private forms of religiosity, including those practiced within one's home, have proven more difficult to monitor and repress. Digital technologies have changed that. As processors, sensors, and cameras have proliferated, the extent of religious life that the CCP can surveil has expanded dramatically.

Consider the following:

> **Religious organizations**. Video and audio surveillance of public mosques, churches, and temples has exploded. Rather than simply shut down a religious school or house of worship, authorities can monitor all activity and individuals within those facilities and sanction undesired behavior or individuals with greater specificity. Video surveillance has become so important to Chinese authorities that they recently shut down a popular church in Beijing after it refused to install internal CCTV cameras.
>
> Yet digital technology has also enabled greater surveillance of underground religious organizations and networks. From video feeds to GPS tracking, authorities have greater ability to detect religious groups that meet and operate covertly. In Xinjiang, for instance, smartphone location data, vehicle location data, checkpoint logs, facial recognition technology, and video feeds from buses, streets, and drones, can be used to identify when individuals in the same religious network meet together covertly, potentially even in real-time.
>
> **Religious identities**. From headwear to jewelry, many religions have customary vestments and adornments that signify religious identity. Surveillance states have long used such markers to track and surveil religious minorities, but digital technologies make such surveillance possible on a larger scale. By feeding machine learning algorithms large numbers of images of religious minorities, Chinese companies such as CloudWalk have developed software that estimates whether a given frame of video contains the image of a religious minority. Although the accuracy of these algorithms is likely poor, they are nonetheless being used for real-time classification by police and security services around China, with authorities being notified when someone who is classified as a Uighur Muslim or Tibetan Buddhist appears on a CCTV feed. Surveillance software that scans for religious identity is particularly problematic in light of legal codes like Xinjiang's recent regulation on extremism, which prohibits clothing and symbols associated with "extremist" religious beliefs and movements.

Religious practices. Historically, religious practices have been difficult to monitor without excessive amounts of manpower, particularly outside of urban areas. Yet as with religious identity, networked video feeds have made it possible to observe religious practices in a far wider range of contexts. For instance, the Sharp Eyes project enables authorized individuals within a community to view feeds not only from public security cameras, but also from smartphones and smart TVs, including those within private residences and homes. Since China's recent counterterrorism law and Xinjiang's "de-extremification regulations" refer only vaguely to religious behaviors that may lead to terrorism and extremism, such systems would make it possible for authorities to detain individuals for privately observing customary religious practices. (In Xinjiang, individuals have been detained merely for possessing recordings of the Quran.)

Religious belief. Compared with monitoring religious identity and practices, monitoring religious beliefs has always been more difficult, because it requires access to an individual's private writing and speech. Yet digital technologies have also made it easier to monitor the religious beliefs an individual expresses and engages with. The smartphone in particular has revolutionized state surveillance of religious belief. Not only are Chinese authorities able to monitor messages on WeChat and other applications, but they can also require individuals to install logging software that tracks all video, audio, and text stored on the phone or accessed online. Chinese officials have already used these techniques to detain individuals merely for texting verses of the Quran.

What makes these new forms of religious surveillance so alarming is that they are being coupled with longstanding forms of mass repression.

To date the most extensive campaigns of repression have come in Tibet and western China. In the former, Chen Quanguo, the Party Secretary for the Tibet Autonomous Region (TAR), implemented the "iron grid" campaign in 2011. Borrowing from the "grid strategy" that was first deployed in Beijing in the lead-up to 2008 Olympics, Chen's program divided Tibetan cities and towns into cells, each of which had a police unit with access to video and communications feeds within the cell. In addition, all Tibetans were required to register with Internet Service Providers under their real identity. Coupled with a dramatic increase in Tibetan police units and an expansion of party offices throughout the region, the surveillance decreased the reported number of immolations and protests within the TAR, but at a significant cost to the freedom and vitality of the Tibetan Buddhist community.

Yet Tibet was just a trial run for what was to come in Xinjiang. In 2016, Chen Quanguo was appointed party secretary of the Xinjiang Uighur Autonomous Region (XUAR). By that time, smartphones and drones had become far more capable than in 2011, and breakthroughs in deep learning had made real-time object detection and facial recognition more feasible. Replicating what he had done in Tibet, Chen quickly established a grid system as part of the broader counter-extremism effort known as the "Strike Hard Campaign." Chen and authorities within the XUAR relied heavily on information technology to tie their surveillance system together. To monitor the movement of Xinjiang's Muslim population, buses were required to have video cameras, vehicles were required to install Beidou satellite navigation systems, personal smartphones were

installed with tracking software, and frequent checkpoints were erected at which DNA samples were taken. To help analyze and monitor the information that was collected, Chen commissioned the Integrated Joint Operations Platform (IJOP) in 2017. The IJOP is now functional and has played an integral role in tracking the movements, activity, and communications of religious minorities in the region. In particular, the IJOP and other surveillance systems have enabled state authorities to monitor and enforce recent counter-terrorism and counter-extremism laws and regulations. Since the regulations are often deliberately vague about which religious behaviors and practices qualify as "extremist," authorities are often able to find data points within the information they've collected to justify internment. As a result of these and related efforts, an estimated 10% of Uighur Muslims have passed through the region's detention camps. There they have been subject not only to forced labor, but also rape, forced sterilization and abortion, and even mental incapacitation.

Although Tibet and the XUAR are the most extreme examples, religious minorities in those regions are not the only groups that the CCP has targeted. The party has also relied on digital surveillance to target Christians, as well as spiritual movements like the Falun Gong. As the legal scholar Eva Pils has noted, "What happens in Xinjiang and what happens to house churches is connected ... Those kinds of new attitudes have translated into different types of measures against Christians, which amount to intensified persecution of religious groups."

U.S. Policy Response

As digital surveillance technologies mature, the appeal of digital authoritarianism is only set to grow. The United States should seek to counter the CCP's digital repression of religion in Tibet and Xinjiang not only to help protect the communities suffering human rights abuses there, but also to deter future campaigns within China and around the world.

Recently the White House signed into law the Uyghur Human Rights Policy Act, co-signed a letter to the United Nations Human Rights Council calling on the CCP to end the detention programs in Xinjiang, and sanctioned Chen Quanguo and other government officials and technology executives responsible for mass repression campaigns.

All of those measures are welcome, but they will not be enough. The United States should also consider the following policies:

> **Pressure Muslim allies**. If the world has remained silent on Xinjiang, that is at least partly because Saudi Arabia, Turkey, Indonesia, and other major Muslim countries have yet to speak out vocally, forcefully, and consistently about the plight of Muslims there. In fact, not only have they not condemned the measures China has taken, but in response to the recent UNHCR letter signed by the United States and other democracies, Saudi Arabia and many Muslim majority countries signed a separate letter condoning China's detention policies. The United States should continue to pressure Saudi Arabia and other Muslim countries to reverse course and more aggressively speak out.

> **International independent monitors.** The CCP has acknowledged the existence of camps in Xinjiang, but insists that they are used solely for educational purposes. The

international community should pressure the CCP into allowing international independent monitors into the region to investigate the camps directly. Since there is evidence that the CCP has begun to transfer some detainees to prisons in response to the concerns raised about the camps, the monitors should be able to visit prisons as well.

Impose targeted export controls. Although China is essential to the global manufacturing supply chain for both processors and sensors, it has struggled to become a world leader in advanced semiconductor manufacturing. In particular, the Chinese technology sector has yet to demonstrate it can design and produce the photolithography machines with which state-of-the-art chips are fabricated. The United States should work with the Netherlands and Japan, the two other democratic countries which produce photolithography machines, in blocking the continued sale of such equipment to China.

Develop international standards. For the United States and other democracies to effectively counter digital authoritarianism, critiquing the irresponsible and unethical use of artificial intelligence by the CCP and other authoritarian regimes won't be sufficient. The United States and its democratic allies must also develop, articulate, and adhere to alternative standards and models for the responsible use of AI and emerging technologies. Further, the United States and its allies must rigorously uphold those standards in their own counter-terrorism and counter-extremism efforts.

2022 Beijing Olympics. As with other authoritarian regimes, the CCP views the Olympics as an opportunity to establish its power and legitimacy on a world stage. So long as the CCP continues to operate mass detention camps and carry out related human rights violations, the United States and other democracies should consider conditioning its participation in the upcoming 2022 Beijing Olympics on the cessation of mass repression in Xinjiang and elsewhere.

The United States can and must push back against the technological surveillance of religion by the CCP, and digital authoritarianism more broadly. As the capabilities of digital surveillance technologies grow, authoritarian regimes will look to the programs the CCP has implemented in Tibet and Xinjiang as a potential model for how to surveil and control religious minorities. We owe it to the victims of religious repression in those regions to ensure that their experiences remain an exception rather than a normalized form of social and political control.