UNITED STATES COMMISSION *on*
INTERNATIONAL RELIGIOUS FREEDOM

COUNTRY UPDATE: CHINA

September 2019

USCIRF's Mission

To advance international freedom of religion or belief, by independently assessing and unflinchingly confronting threats to this fundamental right.

Religious Freedom in China's High-Tech Surveillance State

By Dominic J. Nardi, Policy Analyst

Executive Summary

During the past decade, the Chinese government has increasingly employed advanced technology to amplify its repression of religious and faith communities. Authorities have installed surveillance cameras both outside and inside houses of worship to monitor and identify attendees. The government has deployed facial recognition systems that are purportedly able to distinguish Uighurs and Tibetans from other ethnic groups. Chinese authorities have also collected biometric information—including blood samples, voice recordings, and fingerprints—from religious and faith communities, often without their consent. The government uses advanced computing platforms and artificial intelligence to collate and recognize patterns in the data on religious and faith communities. Chinese technology companies have aided the government's crackdown on religion and belief by supplying advanced hardware and computing systems to government agencies. In response to these developments, several members of the U.S. Congress have called for greater restrictions on the export of advanced technology to China. This country update provides a brief overview of the types of technology implicated in religious freedom abuses in China, with examples from specific Chinese companies, as well as the current state of U.S. policy.

Introduction

The Chinese government's ongoing crackdown on religion or belief has reached nearly unprecedented scale and scope. Under President Xi Jinping, Chinese authorities have:

- Detained between 800,000 and two million Uighur and other Muslims for reeducation in internment camps in the Xinjiang Uighur Autonomous Region;
- Seized control of key Tibetan monasteries and expelled thousands of monks and nuns;
- Arrested thousands of Christians and church leaders who refused to join the state-sanctioned church;
- Intensified a campaign to eradicate the Falun Gong and repress other banned groups, such as the Church of Almighty God; and
- closed or demolished dozens of Buddhist and Taoist temples.

www.USCIRF.gov
@USCIRF
Media@USCIRF.gov

732 N. Capitol Street, NW, Suite #A714
Washington, DC 20401
202-523-3240 (p) 202-523-5020 (f)

Accordingly, in 2019, the U.S. Commission on International Religious Freedom (USCIRF) again *recommended* that the U.S. Department of State designate China as a "country of particular concern" (CPC) under the International Religious Freedom Act of 1998.

The Chinese government's violations of religious freedom are unique because of the extent to which it has relied upon advanced digital and biometric technologies to effectively create a surveillance state. At a July 2018 *Congressional-Executive Commission on China* (CECC) hearing, then U.S. Ambassador Kelley E. Currie *testified* that:

> Chinese authorities have constructed a highly intrusive, high-tech surveillance system in Xinjiang, which many experts fear will be extended throughout China. This system includes thousands of surveillance cameras, including in mosques; facial recognition software; obligatory content-monitoring apps on smartphones and GPS devices on cars; widespread new police outposts with tens of thousands of newly-hired police and even Party personnel embedded in people's homes; and compulsory collection of vast biometric datasets on ethnic and religious minorities throughout the region, including DNA and blood samples, 3-D photos, iris scans, and voiceprints.

Although certain parts of the mass surveillance apparatus have been automated, the system still requires significant manpower to collect and review data. In Xinjiang alone, the local government has more than one million officials who regularly monitor and interrogate the Muslim population.

Surveillance Cameras and Facial Recognition

In 2015, China's National Development and Reform Commission launched a program called **Sharp Eyes** with the goal of achieving 100 percent video coverage of "key public areas" and "key industries" by 2020. This marked an expansion of a 2005 public surveillance program called **Skynet**, which has led to the installation of hundreds of millions of cameras across the country. The government has justified this mass surveillance as necessary to stop crime, but cameras have also been installed to monitor the exterior and interior of houses of worship. Cameras have even been installed in the pulpits of some churches, allowing authorities to identify who attends services. Camera coverage is particularly thorough in Xinjiang and Tibet.

Hangzhou Hikvision Digital Technology Co.–a Chinese company–is the largest supplier of surveillance cameras in China. According to *media reports*, Hikvision won a contract with the Xinjiang regional government that includes the provision of cameras that would monitor 967 mosques in a single county in southern Xinjiang. It has also won contracts with at least two counties to provide panoramic cameras and surveillance systems within the internment camps.

Facial recognition technology has been integrated into much of this surveillance network and trained to identify Uighurs and Tibetans. Although facial recognition technology does use features like skin tone and face shapes to sort imagery in photos or videos, it must be programmed by humans to categorize people based on race or ethnicity. Chinese police outside of Xinjiang have started using facial recognition technology to identify and target Uighurs, and there are indications they might soon target Tibetans.

Biometrics and DNA Databases

For several years, Chinese researchers under the supervision of the Ministry of Public Security have been rapidly creating a national DNA database of Chinese citizens. Authorities have sometimes employed coercion to obtain DNA samples. All Xinjiang residents between the ages of 12 and 65 are forced to undergo medical examinations that include the collection of blood samples, images of irises, voice recordings, and fingerprints. In some cases, authorities have conducted these examinations in the internment camps, while in others authorities called Uighurs to police stations to undergo the exam. Several Uighurs have *testified* they did not feel at liberty to refuse the exam or withhold consent.

iFlytek Co.–a Chinese company–*specializes* in speech and speaker recognition and produces an estimated 70 percent of all speech-recognition technology in China. It has helped the Ministry of Public Security to build a national voice pattern database and is believed to be working on a pilot surveillance system that can automatically identify targeted voices in phone conversations. In advertising material, the company claims that its systems can handle minority languages, including Tibetan and Uighur.

In 2018, members of Congress and human rights organizations began to publicly criticize **Thermo Fisher Scientific, Inc.**—a U.S. lab equipment company—for selling DNA sequencers to the Chinese Ministry of Public Security and authorities in Xinjiang. The firm's Applied Biosystems instruments (ABI) Genetic Analyzer can be used to help scientists determine a person's ethnicity from a DNA sample. It is believed that Chinese authorities have been using the technology to track Uighurs. On February 20, 2019, the company *announced* that it would no longer sell its equipment to government authorities in Xinjiang and that it would work with U.S. officials to ascertain how its technology was being used in China.

Databases and Artificial Intelligence

Artificial intelligence (A.I.) systems can combine information from video surveillance, facial and voice recognition, GPS tracking, and other data to recognize patterns of interest to security officials. Chinese tech companies are competing to build methods for automated policing that use algorithms to look for suspicious patterns in social media usage and computer-vision software to track ethnic and religious minorities across the country. According to *experts*, the Chinese government's use of artificial intelligence to track Uighurs and Tibetans is the first known example of a government intentionally using A.I. for racial profiling.

CloudWalk and other Chinese companies have been directly linked to the government's mass surveillance of religious minorities. For example, CloudWalk marketing materials claim its facial recognition systems can recognize "sensitive groups of people," including Uighurs or Tibetans, and send alarms to law enforcement.

Residents in Xinjiang are required to install software on their mobile phones that collects data and makes it available to Chinese authorities. In major urban areas, police use checkpoints—erected every few hundred yards—to scan phones, interrogate commuters, and conduct other security checks. In May 2019, *Human Rights Watch* revealed that it had reverse-engineered a phone app used by Xinjiang police called the **Integrated Joint Operations Platform (IJOP)**, which aggregates the data gathered from phones and flags those deemed of interest. The app targets 36 "person types" for special attention, including individuals who collected money or

materials for mosques "with enthusiasm," preach about Islam without state authorization, follow a blacklisted religious scholar, or go on the hajj (pilgrimage to Mecca) without permission.

SenseNets Technology Ltd.–a Chinese company–experienced a data leak in early 2019, which provided some insight into the capabilities of Chinese surveillance firms. The SenseNets database logged exact GPS coordinates on a 24-hour basis and, using facial recognition, associated that data with sensitive personal information, including national ID numbers, home addresses, photographs, and places of employment. According to *reports*, at the time, the firm was tracking the movements of more than 2.5 million people in Xinjiang. The exposed data also showed approximately 6.7 million location data points linked to specific individuals, all of which were gathered within 24 hours and tagged with descriptions such as "mosque," "internet café," and other places where surveillance cameras were prevalent.

In July 2019, a team of journalists from the *New York Times* and other media outlets *published* a report about an app called **Fengcai**—produced by a subsidiary of the Chinese telecommunications company **FiberHome Networks**—that Chinese border authorities routinely install on smartphones belonging to travelers entering from Central Asia. The app checks content on each phone against a list of more than 73,000 documents, pictures, videos, audio recordings, and other items. Although some of these items are related to known terrorist groups—such as Islamic State of Iraq and Syria (ISIS) training materials—the list also includes items related to mainstream and nonviolent religious practice, such as audio recordings of Qur'an verses recited by prominent clerics and writings by the Dalai Lama.

Current U.S. Policy Responses

Within the past year, various actors within the U.S. government have begun to track and respond to concerns about the role of advanced technology in China's suppression of religious freedom. In particular, members of Congress have raised concern that technology, information, and capital investment provided by U.S. companies has enhanced the Chinese government's capacity to monitor and harass religious and ethnic minorities.

- On September 12, 2018, the then chairs of the Congressional-Executive Commission on China (CECC) sent a *letter* asking the U.S. Department of Commerce to expand the U.S. government's *"Entity List"* for export licenses to include Chinese government entities in Xinjiang, as well as any businesses profiting from the expansion of the government's increase in security spending. The Department of Commerce is currently determining the appropriateness of additional end-user restrictions for Xinjiang police and security forces.
- In *August 2018* and in *April 2019*, bipartisan members of Congress sent letters to the Trump administration urging it to blacklist Chinese companies that have been complicit in and profited from religious freedom abuses in Xinjiang. The letters specifically mentioned Hikvision and Dahua Technology Co.
- On November 19, 2018, the Commerce Department issued a notice *(83 FR 58201)* of a proposed rule-making on "controls for certain emerging technologies," which would include additional export restrictions on A.I., biometrics, and advanced surveillance equipment.
- In January 2019, the Uyghur Human Rights Policy Act (*H.R. 649*/*S. 178*), was introduced in both the House of Representatives and the Senate. If passed, the act would require the Director of National Intelligence to provide a report to Congress about the transfer or development of technology used by Chinese authorities to detain and monitor Uighur Muslims. On September 11, 2019, the Senate *adopted* the bill by unanimous consent.

- In February 2019, the Uighur Intervention and Global Humanitarian Unified Response Act *(H.R. 1025)* was introduced in the House and would increase restrictions on export licenses for advanced surveillance and other technology that could aid or abet abuses of religious freedom and related human rights in Xinjiang.
- In June 2019, members in both the House and Senate introduced the China Technology Transfer Control Act of 2019 *(H.R. 3532/S. 1459)*. If passed, the act would potentially increase export restrictions on technology used by the Chinese government to perpetrate religious freedom and other human rights violations.
- In July 2019, two House members introduced a resolution *(H.Res. 493)* to condemn the Chinese government's persecution of Christians, including efforts to install cameras on church property.
- On July 18, 2019, at the Second Annual Ministerial to Advance Religious Freedom, the United States and the governments of several other countries signed a *statement* renouncing and deploring the use of surveillance technologies in suppressing religious freedom.

According to *media reports*, the Trump administration has considered using its authority under the *Global Magnitsky Human Rights Accountability Act* to impose sanctions against Chinese officials responsible for religious freedom abuses in Xinjiang. Any such action has reportedly been delayed until the conclusion of trade negotiations with the Chinese government. USCIRF has *recommended* the use of targeted sanctions like the Global Magnitsky Act against Chinese officials and agencies that have perpetrated or tolerated severe religious freedom violations, including Chen Quanguo, Communist Party Secretary in Xinjiang and Politburo member, among others.

Conclusion

Although the Chinese government's crackdown on religion and belief is not a recent development, the government's ability to harness surveillance, biometric, and artificial intelligence technology has facilitated and exacerbated religious freedom violations. This high-tech surveillance network provides Chinese security officials with unprecedented amounts data about target populations, particularly Uighur Muslims and Tibetan Buddhists. Chinese advocates of comprehensive surveillance claim that it can help deter crime or violent extremism, but the system is not narrowly focused on such activities. Instead, the government uses the surveillance network to monitor commonplace religious behavior, houses of worship, and specific religious minorities, regardless of their criminal record. In Xinjiang, concern of surveillance is so prevalent that many Muslims fear to attend prayer services in mosques. In taking this sweeping approach to surveillance, the Chinese government is effectively treating religion itself—as well as religious followers—as a potential security threat.

UNITED STATES COMMISSION *on* INTERNATIONAL RELIGIOUS FREEDOM

Professional Staff

Harrison Akins
Policy Analyst

Ferdaouis Bagga
Policy Analyst

Keely Bakken
Researcher

Dwight Bashir
Director of Research and Policy

Elizabeth K. Cassidy
Director of International Law and Policy

Patrick Greenwalt
Researcher

Thomas Kraemer
Director of Operations and Finance

Kirsten Lavery
International Legal Specialist

Jason Morton
Policy Analyst

Tina L. Mufford
Deputy Director of Research and Policy

Dominic Nardi
Policy Analyst

Javier Pena
Communications Specialist

Jamie Staley
Senior Congressional Relations Specialist

Zachary Udin
Research Assistant

Scott Weiner
Policy Analyst

Kurt Werthmuller
Policy Analyst

The U.S. Commission on International Religious Freedom (USCIRF) is an independent, bipartisan federal government entity established by the U.S. Congress to monitor, analyze, and report on threats to religious freedom abroad. USCIRF makes foreign policy recommendations to the President, the Secretary of State, and Congress intended to deter religious persecution and promote freedom of religion and belief.

www.USCIRF.gov
@USCIRF
Media@USCIRF.gov

732 N. Capitol Street, NW, Suite #A714
Washington, DC 20401
202-523-3240 (p) 202-523-5020 (f)