As the world becomes more technologically advanced, some governments are harnessing developments such as facial recognition software, GPS tracking, and other innovative software applications in city-wide surveillance systems to evaluate traffic, collect data, and in some cases, monitor citizens. Although this new technology can increase public safety by better tracking and identifying criminal activity, it also can erode civil liberties by targeting vulnerable populations and systematically implementing mass surveillance and control. Actions by the Chinese government in China’s Xinjiang region are an example of the dark side of surveillance.

Located in northwest China, the Xinjiang Uighur Autonomous Region (XUAR) is home to several ethnic minority groups, the largest of which is the Muslim Uyghurs. The region has been subject to tension in recent years because the Chinese government blames Islamist militants and separatists for conflicts in Xinjiang, whereas rights groups claim that the government represses religious freedom and enforces unfair ethnic policies. In March 2017, China passed a law banning a wide range of activities deemed “manifestations” of extremism, as part of the government’s campaign against what it considers the rising threat of terrorism and separatism in Xinjiang. Mass surveillance and security made possible by advanced technology has helped enable this campaign. In 2017, security and surveillance spending in XUAR almost doubled, and Xinjiang’s security costs have increased 10-fold in the past decade, outpacing the rest of the country. New York Times correspondents recently visited Kashgar, a city in XUAR, where they documented surveillance cameras and security checkpoints at every corner, including inside mosques, and noted the confiscation of cell phones by Chinese authorities to ensure that people have downloaded compulsory software that monitors calls and text messages.

This level of surveillance has empowered the Chinese government to undertake much darker repression tactics in XUAR. In March 2019, an independent researcher estimated that up to 1.5 million Uyghurs and other Muslims have been held in so-called reeducation centers in Xinjiang, calling the detentions an “attempt to eradicate independent and free expressions of the distinct ethnic and religious identities in Xinjiang.” The Chinese government first denied the existence of the centers before officials started referring to them as “vocational...
education and training programs” in October 2018 and then officially named them “vocational training centers” in March 2019. Shohrat Zakir, chairman of the Xinjiang government, dismissed reports that the centers were concentration camps or reeducation camps, instead claiming that they were like boarding schools where students live and eat for free. This account differs from those of UN officials, human rights organizations, and independent journalists, who report that Chinese authorities have extralegally sent people to detention facilities, where they are subjected to forced political indoctrination, renunciation of their faith, mistreatment, and in some cases, torture. In a video that Chinese state television posted showing a class of Uyghurs in the Xinjiang facilities, journalists and human rights activists pointed out surveillance cameras and microphones, demonstrating the technology used to monitor people in cities also permeates the reeducation centers.

The reports of activities in Xinjiang also have prompted attention from U.S. lawmakers. On March 4, 2019, members of Congress wrote a letter to Secretary of State Mike Pompeo urging the Trump administration to take strong measures in response to the Chinese government’s human rights abuses, stating that “of particular concern are reports of U.S. companies that may be contributing to Beijing’s persecution of Uyghurs through their support or commercial ties to Hikvision and Dahua—two Chinese tech giants that have profited from the surge of security spending in Xinjiang.”

Since 2016, Hikvision and Dahua have won $1.2 billion in surveillance project contracts with Xinjiang, and two of Hikvision’s projects were advanced camera systems for detention camps and mosques. These contracts reveal how intertwined Chinese tech companies are with China’s surveillance state, as these companies are providing the technology that makes it possible for the government to repress its people. This February, greater attention was brought to these partnerships when a data leak revealed that SenseNets, a Chinese facial-recognition technology company, collected approximately 6.7 million GPS coordinates linked to names, ID card numbers, and birth dates, and tagged with descriptions such as “mosque,” “hotel,” “internet cafe,” and other locations where surveillance cameras were likely to be placed.

Still, despite warnings, U.S. companies continue to hold investments in Hikvision, as many investors seem to be ignoring Xinjiang’s detention camps due to the profitability of the surveillance industry in China. Although customers of Hikvision may feel that they are purchasing products from a private business, a controlling share of the company is owned by the Chinese government, which should raise serious human rights and national security concerns. These concerns are further heightened as ties between U.S. companies and the Chinese surveillance state go beyond financial investment in Hikvision. Firms in the United States are lending expertise, reputational credibility, and technology to Chinese surveillance companies, and the exact details of these collaborations are not often transparent.
On March 13, 2019, Secretary Pompeo spoke upon the release of the State Department’s 2018 country reports on human rights, mentioning that Uyghurs are “interned in reeducation camps designed to erase their religious and ethnic identities.”

Although the Trump administration calling out China for its human rights abuses is a necessary start, there is still the failure to mention the problem of U.S. companies potentially contributing to these human rights abuses.

This April, members of Congress sent a letter to Secretary Pompeo, Secretary of Commerce Wilbur Ross, and Secretary of Treasury Steven Mnuchin arguing that words were not enough and urged the Commerce Department to expand its “Entity List” to include entities that have provided technology, training, or equipment to Xinjiang officials in mass detentions and surveillance to ensure that U.S. companies are not assisting in the policing systems used in the Xinjiang region. The Entity List comprises certain foreign persons who are subject to license requirements for the export of specified items because they have engaged in activities contrary to U.S. national security and/or foreign policy interests. Lawmakers also argue that the United States should establish strengthened disclosure requirements to alert American investors about Chinese enterprises that are complicit in human rights abuses.

Although the Trump administration calling out China for its human rights abuses is a necessary start, there is still the failure to mention the problem of U.S. companies potentially contributing to these human rights abuses.

Despite some members of Congress and the State Department bringing the issue to light, the Trump administration is still paying too little attention to the danger of ties between U.S. firms and the Chinese surveillance state. If the United States continues to ignore the contributions of U.S. funds and expertise to China’s surveillance apparatus, then it bears some responsibility for the abuses occurring in XUAR. This administration needs to step up and prioritize Xinjiang in U.S.-China relations and foreign policy.

Kayden McKenzie is a former intern with the Office of External Relations at CSIS.
ENDNOTES


2. Ibid.


19. Congress of the United States, Letter to Secretary of State Mike Pompeo, Secretary of Treasury Steven Mnuchin, and Secretary of Commerce Wilbur Ross.