Senate Foreign Relations Committee

"Rule by Fear: 30 Years After Tiananmen Square"

Testimony of Sophie Richardson, China Director, Human Rights Watch
June 5, 2019

Chairman Risch, Ranking Member Menendez, members of the Committee, thank you for inviting me to testify on this somber anniversary.

Human Rights Watch began reporting on human rights violations committed by the Chinese government in the mid-1980s, and while many of us had hoped that the government's greater interactions with the international community and institutions over the subsequent years would eventually lead to greater respect for human rights, the reality is the reverse: under President Xi Jinping, not only is the state carrying out gross human rights violations, including heightened repression of peaceful activists and the arbitrary detention of one million Turkic Muslims in Xinjiang, it is also aggressively attempting to undermine international institutions critical to protecting the human rights of people around the world.

We now know that the 1989 Tiananmen Square Massacre was not an aberration, but an expression of deep-seated authoritarianism embraced by successive administrations in Beijing. The US response to Tiananmen was strong and principled, not just in rhetoric, but in actions. Over time, however, the fate of the sanctions imposed by the US in response to Tiananmen represented a wavering commitment to pressing for reform in China: those sanctions have been slowly eroded on paper, superseded by business interests, and are hardly reflective of Chinese authorities' technological prowess. The sanctions, which were designed to limit the export of "equipment or instruments related to crime control and detection," meant that the US could not sell gear, such as handcuffs. But they do not limit the export of the kinds of technology Chinese police now deploy to maintain "public order" – equipment like DNA sequencers, the sale of which remains permissible under US law.

Our research is only a snapshot of an evolving system of mass surveillance: these systems are generating massive datasets – unprecedented in human history – of personal information, people's behavior, relationships, and movements. The Chinese police are researching ways to use such information to understand in a more fine-grained way how people lead their lives. The goal is apparently to identify patterns of, and predict, the everyday life and resistance of its population, and, ultimately, to engineer and control reality.

Human Rights Under President Xi Jinping

Since President Xi assumed leadership as the Chinese Communist Party (CCP) general secretary in late 2012, his government has actively sought to roll back all of the modest human rights gains made over the previous decades.

Inside China, Xi's government unleashed a ferocious crackdown on independent civil society, arbitrarily detaining and prosecuting, on harsh and baseless charges, human rights lawyers, writers, journalists, and feminist activists. Repression of ethnic minorities and religious communities has grown exponentially, leading to the current crisis in Xinjiang. The government has adopted a slew of blatantly abusive laws, many of them in tension with China's international obligations and its own Constitution. It has killed off legal reform, strengthened the Party and Xi's control over state institutions; in March 2018, the CCP removed term limits on his presidency. Space for any independent activism or peaceful criticism is virtually gone, perhaps best embodied by the July 2017 death under guard of 2010 Nobel Peace Prize laureate Liu Xiaobo, or the dramatically shrinking space for human rights in Hong Kong.

Outside China, Xi's government has aggressively engaged in undermining key international human rights institutions, particularly at the United Nations. Beijing's trillion-dollar Belt and Road Initiative has no human rights safeguards; its development banks, including the Asian Infrastructure Investment Bank, are notoriously weak in this regard. Human Rights Watch has detailed Chinese government and Communist Party efforts to limit academic freedom and undercut labor standards outside China. As important, Beijing tries to control and intimidate diaspora communities, ranging from pressuring governments to forcibly return people seeking asylum to censoring WeChat communications between democratically elected representatives and their constituents.

Mass Surveillance Technology Inside – and Outside – China

Among the most disturbing aspects of Xi's rule and the current situation: Chinese authorities' development and deployment of surveillance technology that aspires to engineer a dissent-free society. Chinese authorities deny people any meaningful privacy rights from the government's prying eyes, and, coupled with a deeply politicized judicial system, the lack of a free press, and the denial of political rights, people across the country have no ability to challenge these developments or even truly understand how society is being transformed until it impacts them – or their families – directly.

What are some examples of this technology? One of the Ministry of Public Security's most ambitious and privacy-violating big data projects is the "Police Cloud" system, which appears to be national. The system scoops up information, from people's medical history, to their supermarket membership, to delivery records, much of which is linked to people's unique national identification numbers. The Police Cloud system aims to track where the individuals have been, who they are with, and what they have been doing, as well as make predictions about their future activities. It is designed to uncover relationships between events and people "hidden" to the police by analyzing, for example, who has been staying in a hotel or travelling together. In effect, the system watches everyone, and the police can arbitrarily designate anyone a threat who

requires greater surveillance, especially if they are seen to be "undermining stability" – an alarmingly ambiguous construct. It's critical to understand that there is no transparency in such a designation, and no way to challenge it – this is not the same as predictive policing in the US.

The Chinese government is also developing a national "social credit system" that rewards "good" behavior and punishes the "bad." At present, it is a blacklisting system in which behaviors the authorities disapprove – from "abnormal petitioning" to eating on the subway – can affect one's ability to obtain services, such as getting mortgages and travelling on high-speed trains. The system already has rights implications. We documented a case in which Li Xiaolin, a human rights lawyer, was put on a blacklist for failing to apologize "sincerely" to a plaintiff in a defamation case. In that case, the penalty was exacted in an arbitrary and unaccountable manner: authorities failed to notify him that he had been blacklisted, leaving him no chance to contest his treatment.

To what extent the social credit system will evolve, and how it will interact with the police systems of mass surveillance, remains an open question. It is important to note that the social credit system and the mass surveillance systems were envisioned as part of the Chinese government's bigger vision for "better" "social management" – meaning, social control.

In December 2017, Human Rights Watch documented Xinjiang authorities' compulsory collection of DNA samples, fingerprints, iris scans, and blood types of all residents in the region between the ages of 12 and 65, in part under the guise of a free public healthcare program. That campaign significantly expanded authorities' collection of biodata beyond previous government efforts in the region, which only required all passport applicants in Xinjiang to supply biometrics. It did not appear that the government has disclosed to the public or to participants, the full range of how collected medical information will be used and disseminated or how long it will be stored, and it appears that people were given little information about the program or the ability to opt out of it. We discovered that a US-based company, Thermo Fisher Scientific, headquartered in Waltham, Massachusetts, had sold DNA sequencers to the Xinjiang Public Security Bureau during this period. After inquiries from Human Rights Watch, members of Congress, and the *New York Times*, the company agreed to stop selling that particular technology in that particular region. However, it remains unclear whether it has adopted due diligence policies that might prevent such problems in the future.

Most recently, Human Rights Watch reverse-engineered an app used by police and government officials in Xinjiang that is connected to a police mass surveillance system, called the Integrated Joint Operations Platform (IJOP), which aggregates information about all residents of Xinjiang under the guise of providing public security. Our research into the app revealed that the authorities consider many ordinary and legal behavior, such as "not socializing with neighbors," "often avoiding using the front door," using WhatsApp, or simply being related to someone who has obtained a new phone number, as suspicious. The app then flags such people for interrogation; some of whom are then sent to Xinjiang's "political education" camps where they are arbitrarily and indefinitely detained until authorities deemed them to have become sufficiently loyal to the Chinese Communist Party.

The consequences of these technologies across China are enormous: the state is now not only able to peer into virtually every aspect of a person's public and private life, but is also clearly using information gained that way to reward and punish people outside any discernible legal scheme. It's not just the case that it's now "suspicious" if you go out your back door instead of your front door in Xinjiang, it's that the authorities can know that and investigate and punish you for it, even though it's legal. You are not only suspicious if you question state policies, your level of suspiciousness is also dependent on who you are related to, who you spend time with.

Like other human rights violations committed by Chinese authorities, tech-related abuses no longer stay inside China. In recent years major Chinese firms have sold surveillance technology and provided training to other abusive governments; in 2014 we documented ZTE's sale of telecom surveillance technology to the Ethiopian government, which used that equipment to monitor its political opponents.[1] iFlytek, one of China's major voice recognition companies, which works with the Ministry of Public Security in building a national voice pattern database, is working with universities in the US;[2] it is unclear whether that cooperation is subjected to due diligence strategies to ensure that that collaboration is not inadvertently contributing to human rights violations. China Electronics Technology Group Corporation (CETC), a state-owned defense conglomerate behind Xinjiang's IJOP system, has numerous subsidiaries.[3] These subsidiaries in turn have joint ventures and research and development partnerships abroad. One of CETC's subsidiaries is Hikvision, a major surveillance camera manufacturer whose products are used around the world, including in the US.

Recommendations

We now find ourselves confronted with a powerful Chinese government willing to deploy extraordinary resources to deny people inside and outside China their human rights.

Human Rights Watch appreciates that many congressional interventions on China and human rights have long been bipartisan and bicameral, and that in recent years members of Congress have stood on principle to protest human rights violations even when administrations would not.

To combat the Chinese government's expanding use of surveillance technology in the commission of human rights violations, we urge the United States to impose appropriate export control mechanisms to deny the Chinese government – and Chinese companies enabling government abuses – access to technologies used to violate basic rights, including by adding companies to existing export control lists, and imposing targeted sanctions under the Global Magnitsky Act against individuals linked to serious violations of human rights. US private companies and public universities working in this sector should be encouraged to adopt due diligence policies to ensure they are not engaged in or enabling serious human rights violations.

It is imperative that Congress keep up the pressure on the administration to promote universal human rights; certainly, your multiple inquiries as to the administration's approach to Xinjiang have helped. This is particularly important when it comes to international institutions that have a

[1] ZTE did not respond to Human Rights Watch's letter of inquiry.

[2] iFlytek did not respond to Human Rights Watch's letter of inquiry.

[3] CETC did not respond to Human Rights Watch's letter of inquiry.

role in protecting human rights, including the United Nations Human Rights Council, which I know can sometimes be difficult for members of Congress to do. It is important for you to recognize that the US withdrawal from that body, in particular, has made it much more difficult to develop international pressure to end to the crisis in Xinjiang, and the Chinese government has moved swiftly to occupy this space.

We urge the swift adoption of the Uyghur Human Rights Policy Act, which I was glad to see recently passed out of this committee, and vigorous implementation of the Tibet Policy Act, the Reciprocal Access to Tibet Act, and the Hong Kong Policy Act – all three regions are under enormous pressure from Beijing and face serious encroachments on human rights.

While there is much work for the US to do to limit Chinese government and Chinese Communist Party encroachments on human rights in the United States, particularly with respect to realms such as academic freedom, those strategies should place at their core protecting the rights of people from China who seek an opportunity to exercise those rights – not make assumptions about or limit them as a result of their nationality or ethnicity. This is a mistake the US has made in the past, and it should not be repeated.

Finally, the US – and ideally members of this body, today – should recommit their support to independent civil society across China. That community is under sustained assault, and it needs sustained attention from the US government – including both Congress and the executive branch. People from that community paid a terrible price at Tiananmen; they have paid it over the past three decades. Yet they have not abandoned the Tiananmen spirit, and neither should the US.