"Techno-Authoritarianism: Platform for Repression in China and Abroad"

Written Testimony

before the

Congressional-Executive Committee on China (CECC)

November 17, 2021

By Geoffrey Cain

Author, *The Perfect Police State: An Undercover Odyssey Into China's Terrifying Surveillance Dystopia of the Future*

Congressional Innovation Fellow, TechCongress

Chairman Merkley, Co-Chairman McGovern and Members of the Commission:

It is an honor to be invited to testify here on China's surveillance apparatus and the threat it poses globally.

Democracies around the world are straddled with a grave and unprecedented problem: the creation of new, totalitarian surveillance technologies, developed faster than we can implement the democratic laws, norms, and checks and balances that will ensure these technologies do not fall into the wrong hands.

Today I will talk about a place where these surveillance technologies have enabled genocide and crimes against humanity. I will talk about the situation of the Uyghur population in China's western region of Xinjiang, where about 1.8 million people have languished in a network of hundreds of extrajudicial concentration camps, out of an ethnic minority population of about 11 million people. Since 2016, the People's Republic of China has engaged in an unprecedented experiment in social control in Xinjiang. It has deployed novel technologies in artificial intelligence, facial recognition, voice recognition and biometric data collection to oppress its people in new ways.

In the twentieth century, genocides took place in gas chambers and mass graves. But in the twenty-first century, modern technology has allowed the People's Republic of China to commit the beginnings of genocide, wiping out a people in silence, through cultural erasure and forced sterilizations, without the use of mass physical violence and killings.

This is all documented in my book, *The Perfect Police State: An Undercover Odyssey Into China's Terrifying Surveillance Dystopia of the Future*, published in June 2020 by the

Hachette Book Group. From August 2017 to February 2021, I was an investigative journalist in China, Turkey and Kyrgyzstan, where I interviewed 168 Uyghur and Kazakh refugees. These refugees consisted of former concentration camp detainees, their family members, American and European diplomats tracking the atrocities, Chinese government officials, academics, former Uyghur technology employees at major Chinese corporations, and former Uyghur intelligence operatives from the Ministry of State Security, an intelligence body.

In December 2017, I made my final visit to Kashgar, the Uyghur heartland, and Urumqi, the regional capital of Xinjiang. Within three days, I was detained and asked to leave. To protect my data, my sources, and my own safety, I have not returned.

Technology, Torture and Genocide

In interviews, Uyghur and Kazakh refugees all told similar stories about the region's descent into a total surveillance dystopia. First and most commonly, they recounted how authorities from the Ministry of Public Security, the Ministry of State Security, and Chinese technology firms such as Huawei, Hikvision, SenseTime, Megvii and others have innovated the technologies that are deployed for a dragnet. The police used these technologies for what interviewees say is system of psychological torture.

When refugees and former camp detainees say "psychological torture," they meant the feeling of constantly being watched, not by humans, but by crude software systems designed to predict future crimes and acts of terrorism, with great inaccuracy. The software platform, known as the IJOP, or the Integrated Joint Operations Platform, gathered data from a myriad of sources, including police input, camera surveillance, and criminal and court histories. It was straight out of the science fiction

movie *Minority Report*, about a police unit that arrests and brainwashes people believed to be future criminals before they have even committed a crime.

Former Uyghur technology workers, from major Chinese companies, told me about how the system worked from the inside. They said that the artificial intelligence used data to train a crude, simple algorithm and find correlations between data points, and then determined who was likely to commit a crime based on a number of unrelated, outside factors. The system sent a "bump" or "nudge" to the smart phones of local police to investigate or detain an individual, for reasons often unclear to the human users of the software. These reasons for detention could be as far-flung as whether or not a resident began a physical exercise routine suddenly, entered their home through the front or the back door, or had the flu and was late for work one day.

Under constant surveillance, sometimes without a human to oversee these decisions, refugees said they were terrified at the prospect of doing anything that diverted from their daily schedules and flagged them as potential criminals. They trained themselves to become like machines or robots, able to answer every police question in a pre-programmed way, repressing their own feelings, thoughts and desires.

At concentration camps, where psychological and physical torture have been well-documented, refugees described fellow detainees as lacking personality and expression, like people who had a memory wipe. Their only way of surviving was to do what the camp guards and teachers said, without question. The surveillance technology was designed to force them to deny their own reality and internalize the thinking of the Chinese Communist Party. By internalizing CCP propaganda, these detainees did exactly what the CCP wanted from them: detainees erased their own internal sense of culture, heritage, community, and upbringing which separated them from the dominant Han Chinese population.

Key Sources

Looking beyond data alone, the personal stories of Uyghur and Kazakh refugees are harrowing and have much to warn us about the misuse of surveillance technologies.

To protect their safety, I granted anonymity to two key interviewees who appeared in my book. They are "Maysem," a young woman now in her thirties from Kashgar, who obtained a master's degree in the social sciences from a university in Ankara. She remains in Ankara as a refugee after being taken to lower-level "reeducation center," followed by a high-security "detention center," in late 2016 for about one week.

Maysem asked for anonymity and for the author to obscure some details of her story because she believes her entire family has been taken to a camp as of late 2017 or early 2018, and remain vulnerable.

The other key anonymous source was "Irfan," who now resides in Turkey and had obtained a mid-senior management position as an information technology (IT) worker at a major Chinese telecommunications firm in Urumqi, his hometown. Irfan asked for anonymity because he was revealing what the PRC would probably consider state secrets, surely leading to the imprisonment of his family in Xinjiang, and his own imprisonment and perhaps even execution should he ever be required to return to China.

Under contract with the Ministry of Public Security, Irfan led teams of IT workers and engineers who, from the late 2000s and early 2010s, began establishing networks of surveillance cameras all over Urumqi. Irfan witnessed the escalating surveillance by the Ministry of Public Security first hand. This included the rollout of dragnet artificial intelligence (AI), facial recognition and voice recognition systems, and digital surveillance camera technology from 2010 to 2015 until his departure from the telecommunications company in 2015.

Irfan also detailed the connivance, complacency and involvement of major Chinese telecommunications firms in creating the surveillance apparatus in Xinjiang. All the firms he detailed have been sanctioned by the U.S. Department of Commerce, a government body that, under both the Biden and Trump administrations, has similarly accused these firms of involvement in human rights abuses in Xinjiang.

I did not grant anonymity to interviewees who had already become public figures and whose stories were available in the public domain, search engines and media websites. One key public interviewee was Yusupjan Ahmet, who came from Karamay, Xinjiang and who had migrated to Turkey as an intelligence operative for the PRC Ministry of State Security.

Yusupjan detailed his life story in a series of hours-long, recorded interviews with the author. He stated that he intended to travel to Afghanistan in the early 2010s to become a jihadist fighter, that he was instead imprisoned, and that the state coerced him into spying on fellow Uyghurs by torturing and threatening his mother.

In 2017, with the help of a former military officer in Pakistan, Yusupjan was flown to Afghanistan where he joined a local Taliban militia, while posing as a jihadist. The Ministry of State Security ordered him to report back on the activities and whereabouts of Chinese citizens, mainly Uyghurs, who had become jihadi combatants in Afghanistan. In 2017, the Ministry of State Security relocated Yusupjan to Turkey, where he was ordered to gather intelligence on the local Uyghur community in Istanbul, Turkey. In particular, PRC intelligence operatives wanted him to infiltrate local Uyghur-owned businesses posing as a young person seeking employment.

PRC intelligence officers told Yusupjan that the Turkestan Islamic Party (TIP), a fundamentalist terror group, had infiltrated the Uyghur community in Turkey, and that his objective was to locate and document these supposedly widespread underground networks. Yusupjan, however, was disillusioned to find no evidence of

widespread infiltration. He found the PRC's claims to be little more than a conspiracy theory designed to justify the mass detention of his fellow Uyghurs back in China.

In 2018, Yusupjan defected from the Ministry of State Security and went into hiding. He relocated to Zonguldak, a small, industrial town in northern Turkey on the coast of the Black Sea. There, he kept a low profile, working as a gas station attendant. Two other Uyghur residents in Zonguldak told the author that while they heard, through local community talk, that Yusupjan was a resident, they knew little about him and his life story. He kept a low profile.

In November 2020, while visiting a friend in Istanbul, Yusupjan was preparing to offer an interview to the BBC. As he left his friend's apartment, a man wielding a gun, reportedly of Azeri (Azerbaijan) background, appeared on the street and shot him twice in the back of the shoulder. Yusupjan survived, but has been hospitalized, close to paralyzed and unable to walk for months.

Exporting the Surveillance State

The technologies are no longer unique to Xinjiang. Chinese companies have made them available for export around the world, posing threats to democracy and rule of law. Mexico, Brazil, Serbia, Singapore, Turkey, Spain and South Africa are all examples of countries that have embraced "Safe Cities" programs, designed by Huawei for surveillance and crime prevention.

While there is nothing wrong with adopting technologies that can stop crime, one legitimate fear is that authoritarian or quasi-authoritarian governments will exploit these systems to seize more power and monitor their political opponents. One study

by the Brookings Institution concluded, "countries that are strategically important to the PRC are comparatively more likely to adopt it, but so are countries with high crime rates."

I will give some examples. The authoritarian government of Uzbekistan, a Central Asian country between China and Russia, announced at a security meeting in May 2019 that it signed with Huawei to develop a Safe Cities system with 883 cameras in the Uzbek capital, Tashkent, to, in Orwellian terms, "digitally manage political affairs." In non-democratic Uganda in sub-Saharan Africa, *The Wall Street Journal* reported in August 2019 that Huawei technicians helped the government access the Facebook pages and phones of opposition bloggers who criticized the president. Huawei denied the allegation.

Denialism of Crimes against Humanity

It is a tragedy that some individuals, companies and governments have chosen to downplay or deny evidence of mass atrocities in the Xinjiang region, sometimes for their own market access to the PRC. Their denials are in line with CCP propaganda.

My research underwent a three-month, rigorous fact-checking process, looking for inconsistencies, omissions and inaccuracies. With a professional fact-checker and a journalist, we compared our own refugee testimonies with the published reports of other refugees, academics and journalists, including research by all the scholars testifying here today. We checked the locations and structures of concentration camps and other locations on Google Maps satellite imagery, in technology company press releases and official reports, and in investigative journalism already published in other

periodicals such as *The New York Times, The Wall Street Journal,* and *Buzzfeed*. We also double-checked Chinese-language media.

How to Take Action

Because of the situation before us, I urge Congress to take action on these points. The following are a sample of possible actions, and are not exhaustive:

- Pass the CHIPS for America Act (H.R.7178). Introduced in the House in 2020. The Act will invest in and incentivize research and development and supply chain security in America's semiconductor industry. Establishing a strong semiconductor supply chain at home, in America, will be key to stopping malign state actors from undermining our democracy through technology.

- Pass legislation that would require the U.S. Department of Commerce Bureau of Industry and Security (BIS) to publish reports on a regular basis for Congress and the public, providing evidence for sanctions of foreign businesses. While BIS already releases reports on sanctions, sometimes they do not offer much detail as to why specific entities have been added to the sanctions list. In October 2021, BIS began amending export controls to cover items used in surveillance and espionage that disrupts networks, a great step in the right direction.

- Pass the Uyghur Forced Labor Prevention Act (HR1155). A similar bill was passed in the Senate in July 2021, and HR1155 has been introduced in the House but has not proceeded. The bill would pressure the PRC to curtail the Xinjiang surveillance dystopia, by blocking goods made with forced labor in Xinjiang, such as clothes and electronic components, from entering the US market.