China's surveillance tech is spreading globally, raising concerns about Beijing's influence

Arjun Kharpal

Surveillance cameras are mounted on a post at Tiananmen Square as snow falls in Beijing, China, on Thursday, Feb. 14, 2019.

Qilai Shen | Bloomberg | Getty Images

China's push to export its surveillance technology via some of its biggest companies, including to liberal democracies, has raised concerns because of the risk of data being siphoned back to Beijing and the growing influence of the Communist Party, experts told CNBC.

The world's second-largest economy has built a vast surveillance state comprised of millions of cameras powered by facial recognition software. The devices, perched on lamp posts and outside buildings and streets, are able to recognize individuals.

Some of China's most valuable technology firms have been involved in such projects across the country. But this technology is now being exported as the nation's technology firms expand their global footprint.

Chinese tech companies — particularly Huawei, Hikvision, Dahua, and ZTE — supply artificial intelligence surveillance technology in 63 countries, according to a September report by the Carnegie Endowment for International Peace think tank. Of those nations, 36 have signed onto China's massive infrastructure project, the Belt and Road Initiative, the report said, adding that Huawei supplies technology to the highest number of countries.

Some of these so-called "smart city" projects, which include surveillance technologies, are underway in Western countries, particularly in Europe, including Germany, Spain and France, according to analysis by the Australian Strategic Policy Institute (ASPI).

I think we don't even quite understand the full scale of the problem that we are dealing with when it comes to Chinese surveillance technology when it is exported.

Samantha Hoffman

fellow at Australian Strategic Policy Institute's Cyber Centre

Experts warned of a number of risks including potential access to data by the Chinese government.

"I think that sometimes there is an assumption that 'oh well when we roll out this technology we aren't going to use it in a negative way, we are using it to provide services or we are using it in a way that is seen as acceptable, socially acceptable in our society,'" Samantha Hoffman, a fellow at ASPI's Cyber Centre, told CNBC's "Beyond the Valley" podcast.

"But actually (we) can't be sure of that because the difference isn't necessarily how the technology is being deployed, but who has access to the data it's collecting," she said. "If it's a Chinese company like Huawei, and that … data goes back to China and can be used by the party in whatever way that it chooses."

Chinese laws and regulations

Hoffman cited laws in China that appear to compel Chinese firms to hand over data to the government, if asked. She did not accuse Huawei of wrongdoing, but just used the company as an example.

Earlier this year, Huawei CEO Ren Zhengfei said he would "definitely say no" to any request for customer data from Beijing.

"I think we don't even quite understand the full scale of the problem that we are dealing with when it comes to Chinese surveillance technology when it is exported. It's not just that other regimes can use it in similar ways, it's that when it's exported the (Chinese Communist) Party can attach its interests as well," Hoffman added.

I think the worse future could be these governments adopting these technologies and adding that arsenal to the existing ones for the control of people.

Maya Wang

China researcher at Human Rights Watch

Nowhere is China's surveillance state more visible than in Xinjiang, home to China's Uighur minority. The territory has made headlines for its detention and "re-education" camps that hold an estimated 1.5 million Muslims, many of them for violating what Amnesty International describes as a "highly restrictive and discriminatory" law that China says is designed to combat extremism.

Maya Wang, a China researcher at Human Rights Watch, focuses on Xinjiang and the surveillance activities there. She warned of the dangers of China's surveillance technology going to authoritarian states.

"I think the worse future could be these governments adopting these technologies and adding that arsenal to the existing ones for the control of people," Wang told CNBC.

Earlier this year, an ASPI report highlighted other concerns from China exporting its surveillance tech, including being able to undermine democracies, get an edge on new technologies and in military areas.

"You know, domestically and globally, it (Chinese Communist Party) plans to use technology as **(a)** way to both protect and expand its power," Hoffman said. "Globally, the implications of that are that the party is trying to reshape global governance in a way that ... will ensure the party's power."

Privacy backlash

Facial recognition technology has already faced backlash around the world.

Last month in the U.S., California lawmakers banned local police from using facial-recognition software in body cameras. The current ban is temporary.

Earlier this year, the Financial Times reported that the European Commission, the European Union's executive arm, was looking at drafting new regulation on the technology. Microsoft CEO also said in January that he would welcome new rules on the use facial recognition.

The FT also discovered that a developer involved in London's King's Cross area had deployed facial recognition cameras without people's knowledge. This drew criticism from Britain's data protection watchdog which said it was "deeply concerned about the growing use of facial recognition technology in public spaces."

Also in the U.K., Liberty — a human rights advocacy group on behalf of a person called Ed Bridges — brought a case against South Wales Police regarding the use of facial recognition. It was seen as one of the first cases of its kind in the world.

Bridges claimed to have his face scanned by the police force and argued there were no legal safeguards in place for the use of the tech.

"That struck me as being an infringement of my privacy," Bridges told CNBC's "Beyond the Valley" podcast. "I am a law-abiding citizen, I was doing nothing wrong, I was just going about my business, and yet here the police were in my home city taking my data."

The judges in the case ruled against Liberty and Bridges, and said they were "satisfied that the current legal regime is adequate," and that the use of the technology did not violate the Human Rights Act.

Bridges told CNBC he would appeal and that he's concerned about the lack of consent from the public.

"The issue this comes back to is around consent … When I'm walking through what is a public space … how many of us have that sort of option to stop and go … 'hang on my face is being scanned, who is doing this, for what purposes?' We've all got lives to lead and I think that's why it's important to challenge the use of technology in the way that we are," he said.

Surveillance and trade war

Chinese technology firms have been the caught in the crosshairs of the U.S.-China trade war.

Huawei, the world's largest telecoms equipment maker, has been blacklisted by the U.S., restricting its access to American technology. Washington has dubbed Huawei a national security risk, saying its gear could be used by Beijing for espionage. The Chinese tech giant has repeatedly denied those allegations.

On Monday, the U.S. government widened its net to add another 28 Chinese entities to a blacklist called the Entity List. Hikvision, a firm that makes surveillance products, is one of those companies. Dahua, which deals with surveillance equipment, was also added to the list.