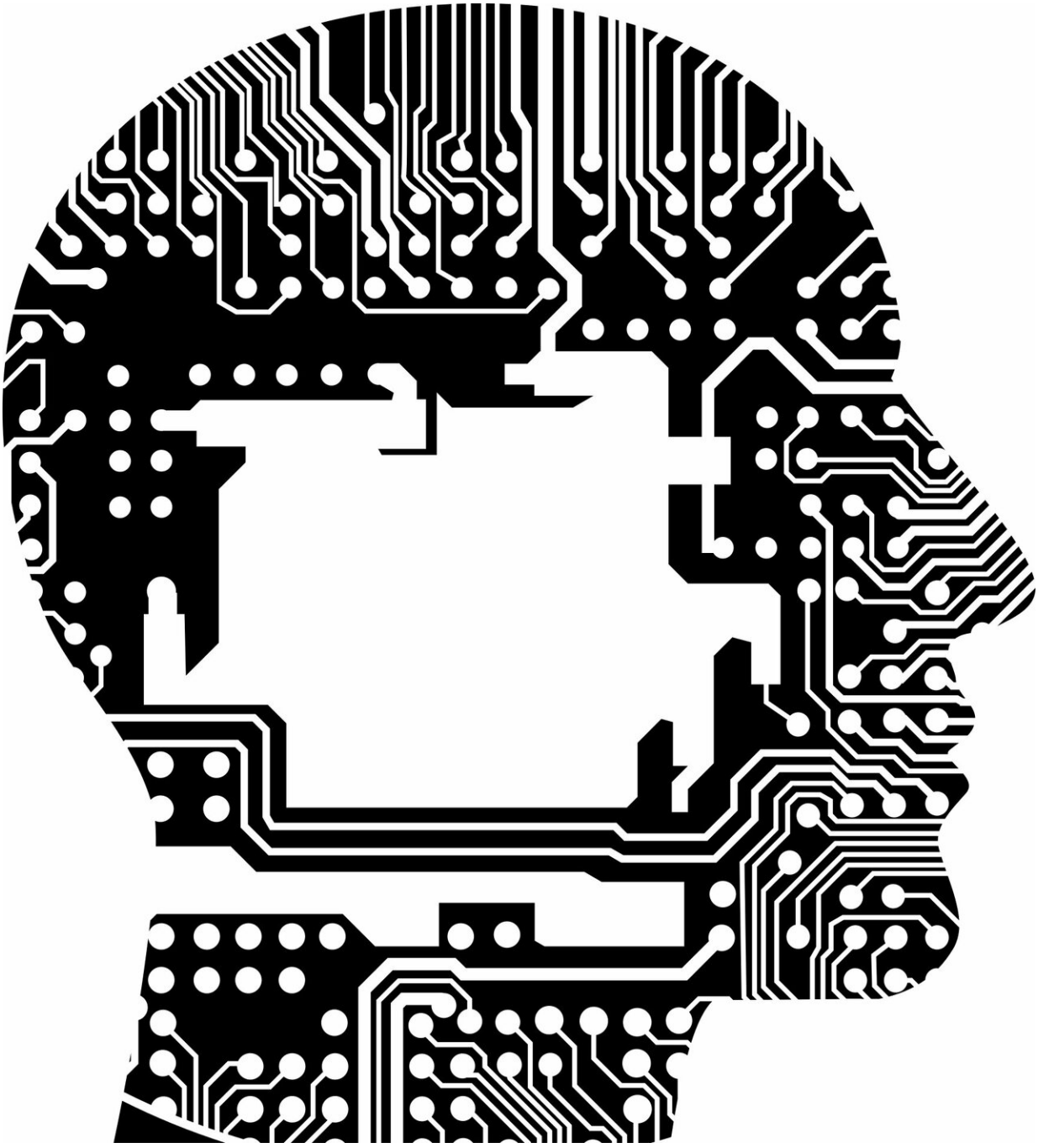
# How artificial intelligence systems could threaten democracy

April 22 2019, by Steven Feldstein



Credit: CC0 Public Domain

U.S. technology giant Microsoft has teamed up with a Chinese military

university to develop artificial intelligence systems that could potentially enhance government surveillance and censorship capabilities. Two U.S. senators publicly condemned the partnership, but what the National Defense Technology University of China wants from Microsoft isn't the only concern.

As my research shows, the advent of digital repression is profoundly affecting the relationship between citizen and state. New technologies are arming governments with unprecedented capabilities to monitor, track and surveil individual people. Even governments in democracies with strong traditions of rule of law find themselves tempted to abuse these new abilities.

In states with unaccountable institutions and frequent human rights abuses, AI systems will most likely cause greater damage. China is a prominent example. Its leadership has enthusiastically embraced AI technologies, and has set up the world's most sophisticated surveillance state in Xinjiang province, tracking citizens' daily movements and smartphone use.

Its exploitation of these technologies presents a chilling model for fellow autocrats and poses a direct threat to open democratic societies. Although there's no evidence that other governments have replicated this level of AI surveillance, Chinese companies are actively exporting the same underlying technologies across the world.

## Increasing reliance on AI tools in the US

Artificial intelligence systems are everywhere in the modern world, helping run smartphones, internet search engines, digital voice assistants and Netflix movie queues. Many people fail to realize how quickly AI is expanding, thanks to ever-increasing amounts of data to be analyzed, improving algorithms and advanced computer chips.

Any time more information becomes available and analysis gets easier, governments are interested – and not just authoritarian ones. In the U.S., for instance, the 1970s saw revelations that government agencies – such as the FBI, CIA and NSA – had set up expansive domestic surveillance networks to monitor and harass civil rights protesters, political activists and Native American groups. These issues haven't gone away: Digital technology today has deepened the ability of even more agencies to conduct even more intrusive surveillance.

For example, U.S. police have eagerly embraced AI technologies. They have begun using software that is meant to predict where crimes will happen to decide where to send officers on patrol. They're also using facial recognition and DNA analysis in criminal investigations. But analyses of these systems show the data on which those systems are trained are often biased, leading to unfair outcomes, such as falsely determining that African Americans are more likely to commit crimes than other groups.

## AI surveillance around the world

In authoritarian countries, AI systems can directly abet domestic control and surveillance, helping internal security forces process massive amounts of information – including social media posts, text messages, emails and phone calls – more quickly and efficiently. The police can identify social trends and specific people who might threaten the regime based on the information uncovered by these systems.

For instance, the Chinese government has used AI in wide-scale crackdowns in regions that are home to ethnic minorities within China. Surveillance systems in Xinjiang and Tibet have been described as "Orwellian." These efforts have included mandatory DNA samples, Wi-Fi network monitoring and widespread facial recognition cameras, all connected to integrated data analysis platforms. With the aid of these

systems, Chinese authorities have, according to the U.S. State Department, "arbitrarily detained" between 1 and 2 million people.

My research looks at 90 countries around the world with government types ranging from closed authoritarian to flawed democracies, including Thailand, Turkey, Bangladesh and Kenya. I have found that Chinese companies are exporting AI surveillance technology to at least 54 of these countries. Frequently, this technology is packaged as part of China's flagship Belt and Road Initiative, which is funding an extensive network of roads, railways, energy pipelines and telecommunications networks serving 60% of the world's population and economies that generate 40% of global GDP.

For instance, Chinese companies like Huawei and ZTE are constructing "smart cities" in Pakistan, the Philippines and Kenya, featuring extensive built-in surveillance technology. For example, Huawei has outfitted Bonifacio Global City in the Philippines with high-definition internet-connected cameras that provide "24/7 intelligent security surveillance with data analytics to detect crime and help manage traffic."

Hikvision, Yitu and SenseTime are supplying state-of-the-art facial recognition cameras for use in places like Singapore – which announced the establishment of a surveillance program with 110,000 cameras mounted on lamp posts around the city-state. Zimbabwe is creating a national image database that can be used for facial recognition.

However, selling advanced equipment for profit is different than sharing technology with an express geopolitical purpose. These new capabilities may plant the seeds for global surveillance: As governments become increasingly dependent upon Chinese technology to manage their populations and maintain power, they will face greater pressure to align with China's agenda. But for now it appears that China's primary motive is to dominate the market for new technologies and make lots of money

in the process.

## AI and disinformation

In addition to providing surveillance capabilities that are both sweeping and fine-grained, AI can help repressive governments manipulate available information and spread disinformation. These campaigns can be automated or automation-assisted, and deploy hyper-personalized messages directed at – or against – specific people or groups.

AI also underpins the technology commonly called "deepfake," in which algorithms create realistic video and audio forgeries. Muddying the waters between truth and fiction may become useful in a tight election, when one candidate could create fake videos showing an opponent doing and saying things that never actually happened.

In my view, policymakers in democracies should think carefully about the risks of AI systems to their own societies and to people living under authoritarian regimes around the world. A critical question is how many countries will adopt China's model of digital surveillance. But it's not just authoritarian countries feeling the pull. And it's also not just Chinese companies spreading the technology: Many U.S. companies, Microsoft included, but IBM, Cisco and Thermo Fisher too, have provided sophisticated capabilities to nasty governments. The misuse of AI is not limited to autocratic states.



Provided by The Conversation

Citation: How artificial intelligence systems could threaten democracy (2019, April 22) retrieved