FACIAL RECOGNITION TECHNOLOGY: USE AND ABUSE CASES IN THE UNITED STATES, CHINA AND HAWAII

BY KENDRICK LEONG, AARON MOSKOVICH, RAE SHIH

Kendrick Leong *is a Master's candidate in the Department of Urban and Regional Planning at the University of Hawaii at Mānoa.*

Aaron Moskovich *is a Staff Sergeant in the United States Air Force and holds a Bachelor of Arts in Political Science from The College of New Jersey.*

Rae Shih *is a legal fellow at the ACLU of Hawai'i working on education policy and civil liberties issues.*

Imagine you and your family are part of a minority ethnic group and practice a minority religion. The government does not support your practices and has developed a facial recognition system that notifies local police when you and your family exit a quarter-mile zone encompassing your home and workplace. Some of your neighbors have been taken to re-education camps, shackled and tortured, and forced to pray in the dominant religion and speak the dominant language. The government is actively trying to eradicate your practices, and to some extent, your ethnic group.

This is not a historical moment or a story from a dystopian novel. In the Indo-Pacific region, China is demonstrating a worst-case deployment of facial recognition technology (FRT) as they utilize it to track citizens and monitor the movements of the Uighur minority group in Xinjiang Province. Surveillance methods include the use of informants, police checkpoints, phone tapping and spyware, and biometric data monitoring.

"That's China though, and the United States is different. That level of minority persecution couldn't happen here under our rule of law."

One should not be so sure. Putting aside current political rhetoric, the US is using FRT in day-to-day monitoring of the public. Law enforcement, sports arenas, airports, and even private companies are using FRT domestically to evaluate risks and monetize personal indicators. Such new uses are under little to no regulation, and the national security narrative is not counterbalanced enough by arguments for the protection of civil liberties and privacy rights.

It may be due to this lack of regulation that FRT has proliferated so widely, so quickly. As of 2016, the Federal Bureau of Investigation has used 16 states' driver's license, booking photos, and/or corrections photos databases in order to identify suspected law offenders. This Next Generation Identification-Interstate Photo System includes 30 million of these photos, and is planned to include voice prints, gait prints, and other biometric indicators.

In addition, local and state law enforcement forces are building their own systems, often contracting with for-profit companies to provide the technology. Indeed, the ubiquity of FRT in both the private and public sector is alarming; Amazon Web Services (AWS) is the cloud vendor for the US intelligence community, 17 agencies and their sub-agencies in total. In 2018, the federal government additionally contracted with Microsoft's cloud service, Azure Government, and its "Face API" software.

FRT, such as these developed and used in the US, are susceptible to Chinese intellectual property (IP) theft. Although Chairman Xi Jinping and President Barack Obama agreed to a baseline

cybersecurity "truce" in 2015, there is growing evidence that China is actively testing boundaries through continued state-sponsored cyber-enabled espionage and theft.

China has stolen American IP through state-sponsored physical theft of hard drives, counterfeiting, and piracy. Furthermore, China's state-sponsored cyber-enabled espionage campaigns target US tech firms, with notable hacks in 2010, 2016, and 2018. The most alarming hacking campaign took place in 2018 when Advanced Persistent Threat 10 (APT10), a Chinese cyber espionage group, targeted US-managed service providers, which store data and passwords for hundreds of US firms. Cracking open these managed service providers would be akin to getting a master key for countless US-developed dual-use technologies.

The development of FRT in the US could be indirectly aiding China's use of FRT on its own citizens when this dual-use technology is stolen or coerced. Chinese state-sponsored IP theft presents the possibility that the FRT China uses to police its own citizens could be traced back to US innovation centers or US-educated talent.

> **"The development of FRT in the US could be indirectly aiding China's use of FRT on its own citizens..."**

Confounding things further is the fact that the Chinese firms involved in data-driven recognition analytics have already been working with the Chinese government to monitor and police its citizenry, attracting international attention. For example, as part of the Belt and Road Initiative, a historically Turkic hinterland in China's northwest is one of two regions that Beijing sees as critical to its long-term economic success. However, the past few decades of insurrection and separatist terrorist activities amongst the majority-Muslim Uighur population in Xinjiang has led Beijing to turn its eye, or more appropriately, its surveillance apparatus, on the region.

Many of us are familiar with the loud whirr of recreational drones. The largest manufacturer of them, DJI, has reportedly signed an agreement with the Xinjiang Public Security Bureau, a Chinese state security apparatus. In the country's developed northeast city of Tianjin, Tiandy Technologies provides facial recognition systems and surveillance cameras to publicly identify and shame jaywalkers. With a population of 1.4 billion, China is an ideal location to hone and perfect the data analytics that underpin successful FRT. Investors have shown interest in underwriting its development, regardless of whose hands the technology ends up in.

Surprisingly, recent developments have shown that maybe good business sense for some Chinese tech firms means staying far away from Xinjiang and the internationally reviled re-education camps located there. SenseTime, the world's most valuable AI start-up headquartered in Hong Kong, recently sold its 51% stake in a joint venture in Xinjiang. SenseTime announced the sale as the result of a strategic reshuffling, but one could point to pressure from its international investors like Qualcomm as the reason behind it, following economic backlash against Chinese tech giants Huawei and ZTE over security and privacy concerns.

While the only thing seemingly holding China back from becoming an AI-fueled Orwellian police state is the economic damage it would do to its tech sector internationally, the US is able to address this issue without making it a matter of dollars and renminbi. Closer to home, legal challenges to the breadth and scope of AI-driven surveillance abound, the latest of which is a Senate bill co-sponsored by Hawaii Senator Brian

Schatz. The bill would institute consumer protections by mandating that consent is given before commercial entities would be able to collect or re-share facial data.

Hawaii's leadership in protecting consumers from the violation of civil liberties incurred by the proliferation of FRT in the US could set a precedent for better conduct throughout the other 49 states and provide stark contrast against the current Chinese abuse of FRT.

The Honolulu Police Department (HPD) currently does not have access to driver's licenses and other sources of facial recognition data, only mugshots. The Hawaii Tourism Authority began a 2016 ad campaign where in-browser software employed FRT to gauge interest in Hawaii-based activities and make recommendations. The ACLU of Hawai'i testified against this action, stating consumers had to give explicit consent for this data tracking. FRT is used at Aloha Stadium as one of many counter-terrorism measures. Law enforcement agencies (LEAs) employ the use of FRT to combat human trafficking in the Hawaiian Islands.

HPD's publicly available usage policy is a step in the right direction, but there needs to exist a clear definition of what type of data facial data constitutes (i.e. biometric, personally identifiable information), what databases HPD and other Hawaii-based LEAs are able to use, and other pain points that can be resolved by the implementation of city, state and federal regulation of FRT.

Disclaimer: All opinions in this article are solely those of the author and do not represent any organization.