HUMAN RIGHTS WATCH

APRIL 6, 2020

The Robots are Watching Us

Published in PEN/Opp

Maya Wang
China Senior Researcher
wang_maya

We used to worry about Terminator-type artificial intelligence robots dominating the human race, but what we are moving toward is more the opposite: humans are being turned into automatons with little freedom to decide what we do.

Across the world, we are seeing a rise of sensory systems monitoring us en masse and round the clock in public and private spaces, whether automatic license plate readers, facial recognition cameras, cellphones tracking location data, or voice assistants in our homes. Each of these "smart" systems promise benefits—less traffic, better security, better maps, better services.

Some of these systems are used in countries with strong human rights protections. In Sweden, for example, the EU privacy law General Data Protection Regulation provides some—albeit limited—protections on how personal data is gathered. These countries also enjoy freedom of expression and the press, public forums where these issues are freely debated.

Most people live in countries with fewer privacy protections, however. Even the US lacks national consumer privacy legislation while the government exercises broad surveillance against citizens and foreigners alike. But the US is also a democracy where increasing awareness about privacy has led states and cities to enact laws like the California Consumer Privacy Act.

Inequalities in human rights protections replicate themselves in privacy protections, with deeply repressive governments—from Zimbabwe to China—actively seeking out new technologies to deepen their assault on rights. In China, not only are there no effective privacy protections, there is also no civil society, free press, or elections. The Communist Party is above the law, maintains a chokehold on the Internet and under Xi Jinping, is increasingly intolerant of dissent.

At the extreme end of this privacy spectrum lies Xinjiang, a region in northwest China with 13 million Uyghurs and other Turkic Muslim minorities. Under the "Strike Hard Campaign against 'Violent Extremism,'" the Chinese government has used technologies to bolster its repression of the Muslim minorities in Xinjiang by tracking virtually their every move, subjecting them to mass arbitrary detention, forced political indoctrination, restrictions on movement, and religious oppression. Credible estimates indicate that one million people are being held in the region's "political education" camps.

Governments' impulse for surveillance is hardly new, but the Chinese government is presenting a new model of social control that, if we do not act now, may become the future for much of humanity.

What does life feel like for Xinjiang's Muslims? Yueming Zhou, a young college-educated woman is—like many people reading this article—cosmopolitan and used to many freedoms. Yueming Zhou was born in Xinjiang but grew up in a Western country. During a summer break, she went back to Xinjiang to visit family. She had used a virtual private network that allowed her to circumvent China's Great Firewall to access her school's website and sign up for classes.

Police soon arrived and took Yueming Zhou to the local police station. They did not tell her what she was accused of, though later she learned that the authorities had detected her use of the private network as they "monitor everything on our phones." The officers took away her passport, handcuffed her, put her into a car, and drove for hours to another Xinjiang city. There, they took her biometric data—including DNA samples, facial images and fingerprints. They then took her to the local "political education" camp.

Yueming Zhou soon found herself down a rabbit hole. The rights she used to have were no more: "I was pushed into a room, where there are six beds in bunk. They searched everything on me, and they made me change into detainee clothes. They then locked the iron door… There was a camera which had a 360-view of the room, a speaker. We were monitored 24/7… When we whispered, we could only speak in Mandarin. We weren't allowed to do anything religious, or say anything that's 'not good' for the government…When we went from our room to the 'classroom,' we had to report our number…"

"There were cameras on the corridors and guards with guns. In the classroom, between the 'teacher' –who stood on the podium—and the 'students,' there was a fence and two or three police officers were also in the classroom. To eat, the cooking staff put rice through a little window; we had to sit on stools and ate with food on our lap."

For months Yueming Zhou had to "learn" Mandarin—she was already a fluent speaker—sing the Chinese national anthem and learn patriotic slogans. She was not to challenge her captors. The more questions you asked the longer you'd be staying," she said her captors told her.

Yueming Zhou was released after five months but her nightmare continued. She was not allowed to leave her hometown. Every week, the police would question her, she had to attend the national flag-raising ceremony on

Mondays and go to night "school" on Thursdays.

A few months into her "release," Yueming Zhou found the courage to venture out to a movie. There was a security checkpoint. When she swiped her ID, the machines made a sound to alert the police, who came and checked her identity. At roads and crossings, cameras scanned Yueming Zhou and other pedestrians' faces. In the police station, she saw computer screens monitoring those crossing the streets with little red squares on people's faces, most likely singling out individuals for further investigation.

The big data system used for monitoring in Xinjiang is the Integrated Joint Operations Platform (IJOP). It acts like a central nervous system for the region's mass surveillance systems, tracking phones, vehicles, and ID cards, and keeping tabs on electricity and gasstation use. It treats many ordinary and lawful activities, even using "too much" electricity, as indicators of suspicious behavior. Some people are singled out for further interrogation and, like Yueming Zhou, are detained or imprisoned.

The system also restricts freedom of movement depending on the level of threat authorities perceive someone poses. The IJOP is connected to the "data doors" installed at some of the region's ubiquitous checkpoints, which send warnings about "problematic" individuals like Yueming Zhou. Together, the high-tech surveillance systems form invisible or virtual fences. This innovative system allows the government to achieve pervasive social control in a region a third the size of Western Europe, while allowing mobility to those deemed "safe" by the authorities, ensuring the provision of pliant labor for the region's economy.

After being held in Xinjiang for 2.5 years without charge or trial, Yueming Zhou got her passport back and left the region.

Xinjiang, while extreme, illustrates how privacy rights are "gateway" rights. When we have no privacy, we risk losing all freedoms. People I interviewed like Yueming Zhou told me how fearful they were and how they had to censor their entire existence. Every facial expression, every piece of clothing and hairstyle, every word they utter, every person they speak to, everything they do—is put under the microscope by their human monitors. But also, quietly and automatically, they are surveilled by the machine sensory systems in their surroundings.

The realities of Xinjiang might be closer than we think. Even for people living in a society with stringent privacy legislation, the laws are not foolproof. Protecting their rights depends on the larger socio-political environment there. As we have seen, societies—including those in the West—can succumb to authoritarian impulses, and a successive government or two with such impulses can flip a democratic society into an authoritarian one.

But unlike past authoritarian states, repressive governments today have at their disposal powerful digital surveillance systems. Companies—including those assisting the Chinese authorities in maintaining an iron

grip over Xinjiang—are selling these wares globally, and at affordable prices, from Kyrgyzstan to Venezuela. Even in the US, Amazon's home surveillance technology, Ring, partners with hundreds of police departments.

We urgently need robust regulatory frameworks that meaningfully restrict the collection, use and storage of biometric data, both by governments and private companies.

Mass DNA collection and analysis—which could reveal not only sensitive information about us but the people we relate to and even what we look like—is one of the Chinese government's tools in Xinjiang. The Chinese government now has the world's largest DNA database, with over 80 million samples, many obtained without informed consent from people unconnected to crimes across the country. In the US, the Justice Department proposed in October to collect DNA samples from detained immigrants. This type of mass collection and indefinite retention of genetic data is a serious intrusion on privacy that should be stopped.

Global alarm about the ubiquity of facial recognition technology for monitoring and identification has been rising, given that it is difficult to alter or obscure one's facial features. While the police—and the companies that supply them—contend that these systems keep us safe, evidence is mixed. Projects adopting the "needle in the haystack" approach—scanning the general public for suspects—have had disappointing results; but those specifically look for missing or trafficked children in orphanages and online sex ads have had some success. Human Rights Watch has urged governments to impose a moratorium on the use of facial recognition until there is sufficient information and debate to decide whether to restrict, or even ban, its use.

Increasingly, companies selling surveillance systems to governments are touting "multi-factor authentication" technologies to "improve accuracy," meaning they are no longer content to identify us just by our faces or voices alone but by a combination of data. In Xinjiang, data doors at some checkpoints not only require people to swipe their smart IDs and scan their faces, but covertly collect people's phone identifying information.

These multi-modal identification systems are particularly dangerous because they are designed to be impossible to circumvent, and as especially invasive and coercive measures can only be justified in rare circumstances. There should also be restrictions on how governments—and companies—can aggregate different sources of data, which can enable them to draw conclusions about people's lives and to manipulate their behavior.

Governments should also re-evaluate "Smart City" projects, which claim to make urban environments more efficient and sustainable, but divulge information on people's identities, movements and habits to either companies out for profit or to agencies that can use the data for ends quite apart from these advertised purposes. As Cory Doctorow points out, alternative models are possible that place human rights at the center of their design and ensure adequate oversight over data collection and utilization.

New technologies are often used before society has a chance to understand and deliberate the costs and benefits. In the late 1960s, the London government began permanently installing surveillance cameras, saying

they were effective crime-fighting tools. But we now see how this helped to normalize ubiquitous public surveillance, a door that once opened led to the dramatically more potent and interconnected systems that are obliterating human freedoms in Xinjiang some 50 years later. We should stop their spread before it is too late.

Related Content

New Leaked Documents Reveal China's Chilling Crackdown on Muslims Unprecedented UN Critique of China's Xinjiang Policies

Region / Country

- Asia
- China and Tibet

Topic

- Technology and Rights
