MERCOLA
Take Control of Your Health

Global Expansion of Mass Surveillance Technology

Analysis by Dr. Joseph Mercola Fact Checked | January 11, 2023

STORY AT-A-GLANCE

- An investigation by The Associated Press reveals pandemic-era mass surveillance technologies are being utilized as instruments of control
- In China, COVID-19 QR codes have been used to restrict movement, protests and other forms of dissent
- In Israel, the Shin Bet security agency used COVID-19 contact tracing technology to send text messages accusing innocent people of acts of violence
- There is fear that COVID-19 mass surveillance technologies will become a measure for widespread social control in which health data, housing information, financial profiles and more are used to create a comprehensive profile of each individual on earth
- The solution to opting out of the madness and protecting your personal privacy and liberties as much as possible is not to voluntarily give up your control and information

Much like air travel was fundamentally changed post-9/11 — justified by national security and the "war on terror" — the world is now profoundly different than its pre-COVID-19 state. Freedoms taken for granted in 2019 were abruptly taken away in 2020, again justified by national security and public health.

But now, even with COVID-19 neutralized, technologies supposedly put in place to monitor and track the virus haven't gone away. On the contrary, they're still being used and expanded throughout the world, revealing that mass monitoring of the global

population wasn't about COVID-19 after all but something much bigger, with the potential to eliminate freedom as we know it.

COVID-19 Technologies Being Used for Control

A year-plus investigation by The Associated Press reveals a concerning trend worldwide in which pandemic-era mass surveillance technologies are being utilized as instruments of control.

"In the pandemic's bewildering early days, millions worldwide believed government officials who said they needed confidential data for new tech tools that could help stop coronavirus' spread. In return, governments got a firehose of individuals' private health details, photographs that captured their facial measurements and their home addresses," AP noted.[1]

Now individuals are finding that data is being used against them — restricting travel and activism, in law enforcement cases and even being shared with spy agencies. As John Scott-Railton with internet watchdog Citizen Lab told AP, "Any intervention that increases state power to monitor individuals has a long tail and is a ratcheting system. Once you get it, is very unlikely it will ever go away."[2]

Surveillance in China Used to Stifle Dissent

In China, citizens were required to install cellphone apps that produce QR codes depending on health status. A green result, based on PCR test results, allows a person to move about freely while a yellow or red result restricted travel or required home confinement. Following widespread demonstrations, the country stated it would no longer enforce national-level health codes to open up travel between provinces.

But Beijing was still requiring local codes for admittance into restaurants, gyms, offices and more. At times over the last three years, entry to a supermarket could be restricted unless a green code was presented, and residents could be quarantined if they were a close contact to someone who tested positive for COVID-19.

The AP investigation, supported by the Pulitzer Center on Crisis Reporting, also revealed that the government used COVID-19 codes to stop dissent:[3]

> *"In early September, former wealth manager Yang Jiahao bought a train ticket to Beijing, where he planned to lodge various complaints with the central government. The night before, a woman he described as a handler invited him to dinner. Handlers are usually hired by state security as part of 'stability maintenance' operations and can require people to meet or travel when authorities worry they could cause trouble.*
>
> *Yang had a meal with the handler, and the next morning Guangzhou health authorities reported a COVID-19 case less than a kilometer from where they dined, he said. Based on city regulations, Yang's code should have turned yellow, requiring him to take a few COVID tests to show he was negative.*
>
> *Instead, the app turned red, even though tests showed that he didn't have COVID. Yang was ordered to quarantine and a paper seal was placed on his door."*

In another example, bank customers who were unable to access their online bank accounts attempted to travel to Zhengzhou to protest. When they arrived at the train station, their QR codes turned red and they were escorted by police to quarantine in the basement. In all 1,317 people traveling to the city to protest the banking commission received red codes — picked up at the high-speed rail train station, the airport and the highway.[4]

Israel's Shin Bet Security 'Repurposing' Surveillance Tech

A similar trend is occurring in Israel, where the Shin Bet security agency repurposed phone surveillance technology used to monitor militants for COVID-19 contact tracing. It's since been repurposed again and has sent text messages accusing innocent people of acts of violence during a period of unrest in May 2021 at the Al-Aqsa Mosque and vowing, "We will hold you accountable."

Majd Ramlawi was among those who received the text. He's a barista at a coffee shop outside the mosque compound, an area peppered with security cameras. "It's like the government is in your bag," Ramlawi told the AP. "When you move, the government is with you with this phone." AP reported:[5]

> *"The Shin Bet's domestic use of the technology has generated an uproar over privacy and civil liberties within Israel, as well as questions about its accuracy. The Ministry of Communications, which oversees Israel's telecommunications companies, refused a request seeking further details submitted for the AP by the Movement for Freedom of Information, a nonprofit that frequently works with media organizations.*
>
> *Gil Gan-Mor, an attorney with the nonprofit Association for Civil Rights in Israel, estimates that hundreds of Arabs in Jerusalem received the threatening message during the unrest and said the mass text message blast was unprecedented. 'You cannot just say to people, 'We are watching you ... and we will get revenge,' he said. 'You cannot use this tool to frighten people. If you have something against someone, you can put them on trial.'"*

Surveillance Overreach Is a Global Problem

The AP obtained documents via the Freedom of Information Act, revealing that countries around the globe are engaging in mass surveillance of their citizens.[6]

- **Mexico —** In the Mexico City suburb Huixquilucan, a surveillance tool was implemented during the pandemic that transmits location, live video and audio of emergency callers to authorities. The technology was said to be necessary for public safety.
- **Pakistan —** The country used military spyware and intelligence services to create an app that identified people infected with COVID-19 as well as those nearby. The Radius Alert function was criticized for privacy violations and leaving users vulnerable to tracking and cyberattacks.

- **South Africa —** Authorities used technology developed to track wildlife poachers for pandemic contract tracing. Movement restrictions were enforced and "smart policing" technologies, including facial recognition and automatic license plate scanners, were implemented in certain cities.
- **Indonesia —** The Health Ministry's eHAC app collected passport numbers, government IDs and COVID-19 testing status from users as a requirement for travel to or within Indonesia. Data from 1.3 million people on the app was left exposed to potential fraud on an open server.
- **Singapore —** Data collected by Singapore's Trace Together COVID-19 app is available to law enforcement to investigate certain crimes designated serious offenses.

In India, meanwhile, facial recognition technologies were used to enforce mask mandates, with police taking pictures of people not wearing the masks, or wearing them incorrectly. Such technologies have been rapidly expanded since the pandemic, and now a patrolling officer can randomly scan a person's face in public and use an app to check for any past criminal activity. According to the AP:[7]

> *"[Hyderabad] Police Commissioner C.V. Anand said the city has spent hundreds of millions of dollars in recent years on patrol vehicles, CCTV cameras, facial recognition and geo-tracking applications and several hundred facial recognition cameras, among other technologies powered by algorithms or machine learning.*
>
> *Inside Hyderabad's Command and Control Center, officers showed an AP reporter how they run CCTV camera footage through facial recognition software that scans images against a database of offenders … Officers decide who they deem suspicious, stoking fears among privacy advocates, some Muslims and members of Hyderabad's lower-caste communities."*

Apps in Australia were also implemented to collect data and notify people if they were in the vicinity of someone who tested positive for COVID-19. But the data was later collected by intelligence agencies. At the local level, citizens used a check-in app that

would notify them if a COVID-19 outbreak occurred in their area. But law enforcement used the data for criminal investigations and contact tracing.

There is fear that the technologies will become a measure for widespread social control, in which health data, housing information, financial profiles and more are used to create a comprehensive profile of each individual on earth.

"Surveillance today is being posed as a technological panacea to large social problems in India, which has brought us very close to China," Apar Gupta, executive director of the New Delhi-based Internet Freedom Foundation, told AP. "There is no law. There are no safeguards. And this is general purpose deployment of mass surveillance."[8]

Pandemic Accelerated Mass Collection of Data in US

In 2020, the U.S. gave $24.9 million to data analytics software company Palantir Technologies to support the U.S. Department of Health and Human Services' COVID-19 response. AP reported:[9]

> *"Documents obtained by the immigrant rights group Just Futures Law under the Freedom of Information Act and shared with the AP showed that federal officials contemplated how to share data that went far beyond COVID-19. The possibilities included integrating 'identifiable patient data,' such as mental health, substance use and behavioral health information from group homes, shelters, jails, detox facilities and schools."*

The U.S. Centers for Disease Control and Prevention also purchased cellphone location data in 2021. The "mobility insights" data revealed the daily locations of at least 20 million cellphones, courtesy of "device IDs" provided by data broker Cuebiq. The ID can link information to individual cellphones and could be used to assess the effects of lockdowns and business closures, among many other more nefarious uses.

As Scott-Railton with Citizen Lab told AP, "What COVID did was accelerate state use of these tools and that data and normalize it, so it fit a narrative about there being a public

benefit. Now the question is, are we going to be capable of having a reckoning around the use of this data, or is this the new normal?"[10]

Are They Watching Your Every Move?

Measures toward authoritarian control and mass surveillance have been increasing worldwide, and in the U.S. Silicon Valley and the national security state are now fused, according to one of my favorite independent journalists, Whitney Webb.[11]

The decades-long wars against domestic dissidence have always involved technology like databases, and now it's progressing to technology like facial recognition apps and widespread use of cameras.

The Chinese government has given billions to the video surveillance company Hikvision, for instance, whose cameras have spread throughout the globe. Their low costs, courtesy of Chinese subsidizing, allowed them to outpace their competition, but concerns have risen that they're ushering in a police state and may act as a "backdoor to Beijing."

The company is a heavyweight in the industry, capable of producing 260,000 cameras daily, which works out to two for every three people born each day.[12] In Britain, 6 million cameras are in use — most of them provided by Hikvision — while the company's presence has also increased, increasing from 70 U.K. staff members in 2018 to 128 in 2021. Among Hikvision's technologies widely used in Britain were heat detection cameras brought on to detect COVID-19 symptoms in 2020.[13]

Worldwide, millions of Hikvision's cameras are in use, concentrating in major cities, including more than 750,000 devices in the U.S.[14] Hikvision also has a U.S. subsidiary called EZVIZ, which is based in California and calls itself a "global smart home security brand" that creates a "safe, convenient and smart life for users through its intelligent devices, advanced AI technologies and cloud services."[15]

Many people have embraced the convenience of "smart" devices in their homes and wearable devices, but there are dangers in intertwining mass surveillance systems with

daily living, whether they're made by Hikvision or another company. The solution to opting out of the madness, and protecting your personal privacy and liberties as much as possible, is to not voluntarily give up your control.

They're counting on you taking your cellphone with you everywhere, and adopting other forms of digital control, like vaccine passports, smart devices and central bank digital currencies. When given the choice to opt in to the latest privacy-sapping technology, don't.

Sources and References

- [1, 2, 3, 4, 5, 6, 7, 8, 9, 10] AP News December 21, 2022
- [11] Sound Cloud, Media Roots Radio August 1, 2021
- [12, 14] The Atlantic October 18, 2021
- [13] The Telegraph May 30, 2022
- [15] EZVIZ, About Ezviz