





**Powered by GLESEC**

# **CYBERSECURITY NEWS CUSTOM REPORT**



## US, Israel, South Korea, and China look at intrusive surveillance solutions for tracking COVID-19

03/19/2020 23:35  Decades of biology go into Google's work on COVID-19 coronavirus Tiernan Ray explains that Google trained a deep learning AI network to figure out the possible structure of some proteins that may play a role in COVID-19, but it was only possible by leveraging decades of government-backed fundamental biological science. Read more: <https://zd.net/2QcxQCS> 

As the global coronavirus (COVID-19) outbreak is leaving its mark across the world, at least four governments are deploying or at looking at implementing privacy-intrusive surveillance systems to track citizens and the disease's spread.

Countries like China and South Korea have already deployed extensive citizen tracking systems, while Israel and the US are preparing similar surveillance measures.

### China

Of all, China leads all countries when it comes to the tracking measures it has currently in use and aimed at dealing with the coronavirus outbreak. Many had been in place for years, such as the Great Firewall, or its ubiquitous street surveillance system. Others, like the Health Code color system and the Hong Kong tracking bracelets, have been stitched together just for the COVID-19 outbreak.

All these systems have been at full throttle ever since the start of the year. Beijing's giant army of censors has used its complete and unhindered control over the Chinese internet and its tech companies to command the local and external narrative surrounding the disease -- although with some mixed results.

In the pandemic's initial stages, censors removed any mentions of an outbreak. Later, as the problem couldn't be ignored, censors started removing all posts or images that critiqued the central government for its late reply in recognizing and dealing with the crisis.

But the biggest role in the Chinese state's surveillance apparatus was played by its almost universal street camera system. First deployed following the Beijing 2008 Olympics, this system has been expanded all over the country's main metropolitan areas and has even been recently upgraded with facial recognition capabilities.

Chinese authorities have been using this system to catch, shame, and fine citizens going outside without face masks and even used it to identify and quarantine individuals who showed symptoms.

But the Chinese government has also been investing in new systems. For example, the local



government has introduced a new scheme called Health Code, which, according to the Guardian, is currently being deployed in over 100 cities.

Chinese citizens can sign up for a Health Code account using their Alipay or WeChat profiles. Once they have a Health Code account, they will be assigned a color code -- red for infected, yellow for quarantined, and green for healthy.

The system allegedly works by scraping a user's Alipay or WeChat account history and mapping a user's travel history. It then weighs other factors like the time spent in outbreak hotspots and if the user had contact with other citizens deemed potential carriers of the virus, and then assigns a health color code.

The system leverages the vast quantities of mobile data and geo-location points Chinese tech companies have been collecting to map infection hotspots and then triage China's population based on their previous interactions.

But if this system seems intrusive, Chinese authorities are taking it one step further in Hong Kong, where they have been using wristbands to track infected locals.

According to a Fortune report, all persons infected or quarantined in their homes were assigned a wristband they had to wear at all times. An older version of this wristband worked paired with a user's smartphone. If the user left his home (quarantine), turned off his phone, removed the bracelet, or the bracelet owner moved too far from his phone, an app on the device would alert the Department of Health, who'd issue a major fine in the owner's name.

The system apparently worked very well, because it received an upgrade this week. According to reports, a new version of the bracelet comes with a built-in GPS tracker to keep tabs on locals wherever they are. Furthermore, the program has been expanded to all travelers as well. If the traveler ventures into an infection hotspot, or has contact with a quarantined or infected local, then the traveler is placed under quarantine as well, all with the data received from the bracelet.

## South Korea

A similarly broad surveillance mechanism was also leveraged in South Korea. According to a report, the Seoul government has heavily relied on CCTV footage, bank card records, and mobile phone data to deal with the outbreak, with extremely good results.

Per reports, the government combined the three data sources to re-trace the steps of all initially infected citizens and then test all the persons they came in contact, aggressively cracking down on infection hotspots before they exploded to envelop the entire country.



## Israel

The Israeli government, which is currently dealing with the early stages of a COVID-19 outbreak, is now working to employ a similar system to the one used in South Korea.

According to Haaretz, the Israeli government passed this week an emergency law that would grant police and the Shin Bet security service access to the entire country's cellphone location data.

Local authorities say they plan to use this information in the same way to South Korea and track down the persons that had contact with known infected hosts, and then notify them via SMS about the next steps they must take.

The Tel-Aviv government also plans to use this cellphone surveillance system to make sure infected users do not leave their quarantine.

The government's decision has not been welcomed with warmth by the Israeli population, though. Many are now fearing that the government may never give up the power it has now granted itself -- the power to track every citizen's location in real-time.

## The US

And discussions on a similar measure are currently also underway in Washington. According to the Washington Post, the White House held meetings last week with Google, Facebook, and several telcos on the topic.

Per reports, the Trump administration wants to know if there a way through which it could gain access to the cellphone location data of all Americans in order to track the spread of COVID-19.

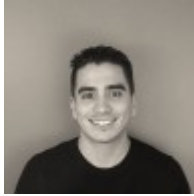
However, things are moving slower in the US, where the White House fears the immense pushback to any Israel-like emergency law, pushback that would come from all sides, such as privacy groups, political rivals, the general public, and the tech companies and telcos themselves.

As some privacy groups and news outlets have already pointed out this week, most countries who have set up surveillance systems in the past have rarely taken them down after their initial purpose has ceased to be an issue, with the US and China being the best examples.

So far, technology has failed to play a role in preventing the coronavirus pandemic, and the virus may end up helping some unscrupulous governments set up surveillance systems that will live years after the current outbreak has died down.



## Will the Coronavirus Normalize Surveillance?



03/18/2020 20:07

Mack DeGeurin Mar 18 · 6 min read



Photo by Bernard Hermant on Unsplash

### The State of Surveillance

**The latest in tech surveillance around the world and where we might be heading.**

**[mack.substack.com](http://mack.substack.com)**

For most people living in Europe and North America, the past two weeks have been a whirlwind.



City shutdowns, stock market collapses, quarantines, empty sports stadiums, canceled music tours, mass panic buying, and tragic tales of suffering are fast becoming the norm. And it seems the most aggressive rollouts of social distancing may indeed work to stop the societal bleeding, but the virus and its fallout will almost certainly get much worse before it gets better.

It's in this bleak context, one mired by despair and laced with anxiety, where people will be forced to make some tough choices. One of those revolves around whether not to use surveillance technologies to stem the tide of new COVID-19 cases.

Several weeks ago in this newsletter, I dived into the surveillance tools the Chinese government used to combat its own disaster. Amongst other things, the Chinese deployed drones equipped with facial recognition software to detect people walking without a facemask on, infrared scanners were stationed at train stations and airports to measure body heat to snuff out people with a fever, and roaming robots reminded potentially at-risk residents to stay indoors.

At the virus's peak, the government even instructed residents to download a monitoring app that appears to have functioned as a surveillance tool, and a new law was rolled through effectively banning negative comments about the government.

If one believes the authenticity of recent data out of China, it appears those extreme measures worked. Week after week, the number of new confirmed Chinese cases shrunk, until finally this Tuesday, The New York Times reported that of the 13 new Chinese cases reported in one day, 12 of them were from travelers visiting from That's pretty remarkable when you consider where China was just a month ago, with hundreds of new cases emerging every day.

This week, in a poignant symbol of how far the country has come, a group of doctors in Wuhan's last emergency hospital hastily built to treat the influx of Coronavirus patients walked out of the hospital for the last time and removed their masks.

While many in the West have questioned whether or not some of China's most extreme limitations on personal freedom in the name of public health could feasibly translate internationally, European and American cities are already following the Chinese playbook in terms of mass social distancing and city-wide shutdowns.

While the US has yet to implement the most extreme forms of surveillance and censorship China used to combat the virus, a growing cadre of developing countries have. In Iran, where the Coronavirus has led to the deaths of over 900 people, including several government officials, a new surveillance app has been created under the guise of tracking new cases.

Millions of Iranian were notified of the app, which claims to diagnose the virus, via a push notification. Here's what that notification said, according to VICE.



“Dear compatriots, before going to the hospital or health center, install and use this software to determine if you or your loved ones have been infected with the coronavirus,” the message said.

The app, of course, does not actually diagnose Coronavirus, but when installed it collect the real-time geo-locations of every person who downloads it. It’s unclear exactly how that data is being used, but the app’s developer, Sarzamin Housmand, has come under fire in the past for helping create an alternative to Telegram — a secure messaging system popular amongst many Iranians — that many believe functions as a surveillance app for the government.

Similarly, this week Israeli Prime Minister Benjamin Netanyahu shocked the world when he revealed the existence of a previously undisclosed secret data tracking system used to monitor suspected terrorists and said the government would begin using it to track Coronavirus cases.

According to reporting in the New York Times, the tool could be used to enforce lockdowns and determine whether or not an infected person had left quarantine. The surprise announcement was met with worry by some privacy advocates who warned the technology could be used to track an individual’s location in real-time or trace a potentially infected person’s metadata to see where they traveled and who they may have come in contact with. Israeli’s fond (potentially through this tool) to have broken quarantine, according to The New York Times, can face up to six months in prison. If that isn’t a surveillance state, I don’t know what is.

The Israel example represents the clearest sign yet that similar surveillance practices may be making their way to Europe and the United States. In fact, some companies are banking on it.

According to Motherboard, Athena Security — a surveillance company whose past work involved firearm detection — claims to have created artificially intelligent thermal cameras that can people and detect fevers. Athena suggests using these cameras at the entrances of grocery stores, hospitals, and voting stations, something pulled directly from the Chinese playbook.

Here’s Athena describing the product on its website.

“Our Fever Detection COVID19 Screening System is now a part of our platform along with our gun detection system which connects directly to your current security camera system to deliver fast, accurate threat detection.

A video of the supposed fever detector also appeared on Youtube.

Elsewhere, an app being developed by the MIT Media Lab claims to track where you’ve been and notify you if you’ve interacted with an infected person. The app, called Private Kit, works by users self-reporting whether or not they’ve become infected. A sick person can share their location with health officials, who will then make the location public.





Private Kit's developers, a ragtag team of MIT, Harvard, Facebook, and Uber engineers, make pains to stress the app's commitment to privacy (hence the name). All data is supposedly encrypted and the app claims it does not share the data with a central authority. Those safeguards are certainly reassuring, but when looking at the app from a broader perspective, it's more evidence of the type of privacy sacrifices gaining traction.

Maybe these are the right decisions. Privacy advocates, even some of the most dogmatic and uncompromising, almost all admit that privacy and personal autonomy must be weighed against the well being of the collective. In situations where nations, or in this case the global community, face extreme health threats, the balancing act between personal freedom and collective health shifts weight.

Self-reporting disease tracking apps like the one above are not totally new, with some flu-tracking variants dating back as far as 2011. As Will Kight reports in , many of the same questions about whether or not such an app would actually be effective and concerns over mass surveillance, existed then as now. The unescapable elephant in the room of course though is Coronavirus.

Society is engaging in a forced upon experiment the likes of which we've never seen. Millions of people all around the world, sick or not, are being told to stay home. Restaurants, bars, movie theaters, concert venues, and every other entertainment staple that's come to coat modern existence has all of a sudden shut off like an exhausted light bulb. How long are people willing to trudge on without these comforts? A month? Two months? More? The longer one imagines society living with this virus, the more likely it appears people may be willing to submit to once-unthinkable surveillance just so they can watch a movie or shoot some pool.

Maybe that's the right conclusion to an uncomfortable trade-off. Maybe not, But either way, one thing seems clear: communities and countries should make those decisions together. Once a surveillance technology is allowed into daily life, it becomes infinity more difficult to retroactively expunge it. Before taking that plunge, conversations and debates over surveillance should dominate the news and friendly banter. That, unfortunately, is far from the case right now.

## The State of Surveillance

**The latest in tech surveillance around the world and where we might be heading.**

**[mack.substack.com](http://mack.substack.com)**

## Privacy in the time of Covid-19





03/19/2020 11:52

Joseph DanaMar 19 · 4 min read



The uneven global response to the Covid-19 outbreak is a window into how governments are grappling with their monopoly on power. But this is not about force or the use of violence. Rather, it is about the competing narratives on privacy in the age of smartphones.

Over the past two decades, technology companies mostly based in China and the United States have created a vast surveillance infrastructure based on smartphone use. In China, that infrastructure is used to maintain control, while in the West it is primarily utilized as an engine for advertising. Regardless of its use, the smartphone is the ultimate vector through which data is collected.



Today, almost everyone has a smartphone. And they are creating a vast amount of information daily. From location data to search history to buying patterns to health records and more, people are walking generators of data. Our social class, background, age and nationality do not matter; we are all connected in the information we create.

But there is a big caveat. Although we create the data, we do not necessarily have the means to access or use it.

Private companies such as Google and sovereign nations such as China have the ability to transform the inchoate data into actionable intelligence. They have designed the algorithms and possess the computing power to turn our random streams of binary zeros and ones into useful material for advertisers, behavioral scientists and, too often, the apparatus of state security.

What does this have to do with the global spread of Covid-19? It's remarkably simple.

Since we all carry smartphones, it is easy to track our every movement and even to predict where we might be at almost any given time of the day, any day of the week. In trying to curb the spread of the virus, some countries have seized on this as a valuable tool.

China's robust (and authoritarian) response to the Covid-19 virus has included the use of its vast surveillance network to ensure that infected people report to state-operated medical facilities. China's ability to contain the virus so quickly is widely credited to this species of Orwellian surveillance.

But China's "socialist democracy" is not a Western one. Israel, on the other hand, likes to believe it is a Western democracy in the Middle East. Yet it has adopted very similar protocols to surveil infected people within its borders.

Using a secret trove of cellphone data culled from its surveillance of Palestinians, Israel's Internet security agency has been tracking people with Covid-19 in an attempt to identify others who may have been infected and need to be quarantined — the technology is promiscuous and does not restrict its attention to just Palestinians.

Used efficiently, the smartphone can track the spread of Covid-19 and inform critical decisions about resource allocation to save lives

The news of this program and its current use shocked many Israelis, leading Prime Minister Benjamin Netanyahu to declare that Israel needed "to maintain the balance between the rights of the individual and the needs of general society." The fact is, Israel has been refining and deploying this technology for years on Palestinians, both in the Occupied Territories and within Israel. Thus the "shock" that many Israelis have declared rings a little false.



Be that as it may, Covid-19 raises important issues about surveillance technology, and well beyond China and Israel. We have the most powerful surveillance infrastructure ever created in history at our disposal. Used efficiently, it can track the spread of this virus and inform critical decisions about resource allocation to save lives.

But will people give governments around the world the power to deploy this powerful technology? And should they?

We have to acknowledge that many — even most — of us already grant this power of surveillance to companies like Facebook and Google. These companies do not answer to anyone but their shareholders. Google, for example, knows more about you than probably your spouse or your doctor. And as the myriad data-privacy scandals over recent years have shown, these companies do not normally operate in your best interest.

That leads to a simple question: Why do we willingly sign over to a Silicon Valley company with a bad track record on data privacy the most intimate details of our lives, but are wary of our own government during a pandemic of possibly historical proportions? There are ample reasons to fault governments' responses to the Covid-19 outbreak, especially in countries like the United States and United Kingdom, but at this grave hour, we need to use every measure we have to combat this virus.

While it might sound frightening to grant governments more power over the intimate details of our lives, the world is facing an unprecedented situation. We have the tools to curb the spread of this virus dramatically.

It is time to think out of the box, because desperate times call for desperate measures. To be sure, we should reassess the ownership interest in our personal data. But that time would be after we have defeated the pandemic.